Related GAO Products

Personnel Security Clearances: Actions Needed to Ensure Quality of Background Investigations and Resulting Decisions. GAO-14-138T. Washington, D.C.: February 11, 2014.

Personnel Security Clearances: Actions Needed to Help Ensure Correct Designations of National Security Positions. GAO-14-139T. Washington, D.C.: November 20, 2013.

Personnel Security Clearances: Opportunities Exist to Improve Quality Throughout the Process. GAO-14-186T. Washington, D.C.: November 13, 2013.

Personnel Security Clearances: Full Development and Implementation of Metrics Needed to Measure Quality of Process. GAO-14-157T. Washington, D.C.: October 31, 2013.

Personnel Security Clearances: Further Actions Needed to Improve the Process and Realize Efficiencies. GAO-13-728T. Washington, D.C.: June 20, 2013.

Managing for Results: Agencies Should More Fully Develop Priority Goals under the GPRA Modernization Act. GAO-13-174. Washington, D.C.: April 19, 2013.

Security Clearances: Agencies Need Clearly Defined Policy for Determining Civilian Position Requirements. GAO-12-800. Washington, D.C.: July 12, 2012.

Personnel Security Clearances: Continuing Leadership and Attention Can Enhance Momentum Gained from Reform Effort. GAO-12-815T. Washington, D.C.: June 21, 2012.

2012 Annual Report: Opportunities to Reduce Duplication, Overlap and Fragmentation, Achieve Savings, and Enhance Revenue. GAO-12-342SP. Washington, D.C.: February 28, 2012.

Background Investigations: Office of Personnel Management Needs to Improve Transparency of Its Pricing and Seek Cost Savings. GAO-12-197. Washington, D.C.: February 28, 2012.

GAO's 2011 High-Risk Series: An Update. GAO-11-394T. Washington, D.C.: February 17, 2011.

High-Risk Series: An Update. GAO-11-278. Washington, D.C.: February 16, 2011.

Personnel Security Clearances: Overall Progress Has Been Made to Reform the Governmentwide Security Clearance Process. GAO-11-232T. Washington, D.C.: December 1, 2010.

Personnel Security Clearances: Progress Has Been Made to Improve Timeliness but Continued Oversight Is Needed to Sustain Momentum. GAO-11-65. Washington, D.C.: November 19, 2010.

DOD Personnel Clearances: Preliminary Observations on DOD's Progress on Addressing Timeliness and Quality Issues. GAO-11-185T. Washington, D.C.: November 16, 2010.

Personnel Security Clearances: An Outcome-Focused Strategy and Comprehensive Reporting of Timeliness and Quality Would Provide Greater Visibility over the Clearance Process. GAO-10-117T. Washington, D.C.: October 1, 2009.

Personnel Security Clearances: Progress Has Been Made to Reduce Delays but Further Actions Are Needed to Enhance Quality and Sustain Reform Efforts. GAO-09-684T. Washington, D.C.: September 15, 2009.

Personnel Security Clearances: An Outcome-Focused Strategy Is Needed to Guide Implementation of the Reformed Clearance Process. GAO-09-488. Washington, D.C.: May 19, 2009.

DOD Personnel Clearances: Comprehensive Timeliness Reporting, Complete Clearance Documentation, and Quality Measures Are Needed to Further Improve the Clearance Process. GAO-09-400. Washington, D.C.: May 19, 2009.

High-Risk Series: An Update. GAO-09-271. Washington, D.C.: January 2009.

Personnel Security Clearances: Preliminary Observations on Joint Reform Efforts to Improve the Government wide Clearance Eligibility Process. GAO-08-1050T. Washington, D.C.: July 30, 2008.

Personnel Clearances: Key Factors for Reforming the Security Clearance Process. GAO-08-776T. Washington, D.C.: May 22, 2008.

Employee Security: Implementation of Identification Cards and DOD's Personnel Security Clearance Program Need Improvement. GAO-08-551T. Washington, D.C.: April 9, 2008.

Personnel Clearances: Key Factors to Consider in Efforts to Reform Security Clearance Processes. GAO-08-352T. Washington, D.C.: February 27, 2008.

DOD Personnel Clearances: DOD Faces Multiple Challenges in Its Efforts to Improve Clearance Processes for Industry Personnel. GAO-08-470T. Washington, D.C.: February 13, 2008.

DOD Personnel Clearances: Improved Annual Reporting Would Enable More Informed Congressional Oversight. GAO-08-350. Washington, D.C.: February 13, 2008.

DOD Personnel Clearances: Delays and Inadequate Documentation Found for Industry Personnel. GAO-07-842T. Washington, D.C.: May 17, 2007.

High-Risk Series: An Update. GAO-07-310. Washington, D.C.: January 2007.

DOD Personnel Clearances: Additional OMB Actions Are Needed to Improve the Security Clearance Process. GAO-06-1070. Washington, D.C.: September 28, 2006.

DOD Personnel Clearances: New Concerns Slow Processing of Clearances for Industry Personnel. GAO-06-748T. Washington, D.C.: May 17, 2006.

DOD Personnel Clearances: Funding Challenges and Other Impediments Slow Clearances for Industry Personnel. GAO-06-747T. Washington, D.C.: May 17, 2006.

DOD Personnel Clearances: Government Plan Addresses Some Long-standing Problems with DOD's Program, But Concerns Remain. GAO-06-233T. Washington, D.C.: November 9, 2005.

DOD Personnel Clearances: Some Progress Has Been Made but Hurdles Remain to Overcome the Challenges That Led to GAO's High-Risk Designation. GAO-05-842T. Washington, D.C.: June 28, 2005.

High-Risk Series: An Update. GAO-05-207. Washington, D.C.: January 2005.

DOD Personnel Clearances: Preliminary Observations Related to Backlogs and Delays in Determining Security Clearance Eligibility for Industry Personnel. GAO-04-202T. Washington, D.C.: May 6, 2004.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: http://www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

2012 Clinger-Cohen Core Competencies & Learning Objectives

December 2012

Contents

Introduction

The Information Technology Management Reform Act of 1996 (also known as the Clinger-Cohen Act and now codified in title 40 of the United States Code) created a wide array of responsibilities for federal agency Chief Information Officers, including developing strategies and specific plans for hiring, training and professional development of the information technology (IT) workforce. In 1997, the first iteration of the Clinger-Cohen Core Competencies was published to create a baseline of information resources management knowledge requirements. Learning objectives were added in 1999 to identify the level of performance desired to be mastered within an academic or experiential environment.

Periodically, the Federal Government reviews this core body of competencies in order to ensure critical knowledge areas impacting information resources management are captured. Changes reflect new statutory and regulatory requirements, as well as areas requiring greater emphasis due to new policies and strategies (e.g., the recently released presidential strategy on Digital Government), continuous changes in technology, and other evolving agency IT/cybersecurity mission requirements. In 2012, new competencies were added for IT Governance, IT Program Management Leadership, Vendor Management, Cybersecurity/Information Assurance Strategies and Plans, Social Media, Cloud Computing, Open Government, Information Collection, and Information Accessibility. Administratively, references were updated and summarized in a separate appendix, and language was streamlined in accordance with the Plain Writing Act of 2010.

The review process was a collaborative effort among 12 federal agencies, academic representatives from the CIO University Consortium, and members from the Industry Advisory Council and federally funded research community and was led and managed by the IT Workforce Committee of the CIO Council.

The 2012 Clinger-Cohen Core Competencies and their associated learning objectives will be used as the foundation for IT course and curriculum development, as well as the development and consistent implementation of IT workforce policy initiatives across the Federal Government. This effort fulfills IT workforce management requirements set forth in Subtitle III of title 40 of the United States Code (U.S.C.) (Clinger-Cohen Act of 1996) and title II of Public Law 107-347 (E-Government Act of 2002, 44 U.S.C. 3501 note).

2012 Clinger-Cohen Core Competencies and Learning Objectives

The Clinger-Cohen Core Competencies reflect a core body of 12 competency areas identified by the Federal CIO Council as fundamental to the effective management of federal technology resources: Policy and Organization; Leadership and Human Capital Management; Process and Change Management; Information Resources Strategy and Planning; IT Performance Assessment: Models and Methods; IT Project and Program Management; Capital Planning and Investment Control; Acquisition; Information and Knowledge Management; Cybersecurity/Information Assurance; Enterprise Architecture; and Technology Management and Assessment. Each of the 12 competency areas has several subordinate competencies and all subordinate competencies have associated learning objectives.

The learning objectives form the foundation for curriculum development by the educational institutions offering approved programs under the CIO University Consortium umbrella. The objectives identify key concepts and capabilities to be taught and can also be used as a professional development guideline for both individuals and organizations. Each individual's professional development roadmap can be achieved through a variety of methods, including formalized academic programs, mentoring, on-the-job training, professional details, and prior experiential assignments.

It is not expected than any one individual would master all management activities contained within these competencies. Areas of concentration would reflect individual job requirements, as well as personal development interests. Additionally, specific technical expertise outside the scope of these competencies may be required based on actual job roles. Federal Chief Information Officers should ensure that the knowledge, skills and abilities represented in each competency in this document are resident within their organization for overall staff productivity.

References listed next to selected learning objectives are designed to guide the learning process but should not be considered all-inclusive. The references cited reflect pertinent statutes, regulations, and policy associated with the given subject matter that are particularly relevant for federal IT employees. A complete listing of references is included in Appendix A.

Finally, individual learning objectives have been mapped to the Office of Personnel Management's Executive Core Qualifications (ECQ) where applicable. Attainment of these qualifications is required for entry to the Senior Executive Service. The mapping is provided to support multi-purpose leadership development for IT management and executive positions.

Clinger-Cohen Core Competencies	Learning Objectives
1.0: Policy and Organization	*General Discussion: The CIO has one of the most cross-cutting positions in government and must be able to work effectively with a wide range of people across multiple organizations. Additionally, the CIO must be comfortable in a fast-changing environment that includes evolving technologies, legislation, policy, and politics.*
Competency 1.1 - Department/Agency missions, organization, functions, policies, and procedures	1.1 LO 1: Describe the varied interpretations of information technology (IT) (e.g., systems data, related peripherals and services); IT focus (operational vs. technical); and IT's typical use in organizational structures.
	1.1 LO 2: List and describe the elements of the CIO's role that are common to all CIOs regardless of their organization's size.
	1.1 LO 3: Define the CIO's role in the Federal Government including: (1) leadership of the IT organization/community; (2) oversight role associated with IT governance; and (3) valued member of the Department's senior leadership team. (See also Competency 1.6 on IT governance.)
	1.1 LO 4: Compare different agency CIO organizational structures against general models available. (See also 1.4 LO 2.)
• OPM ECQ 1	1.1 LO 5: Using metrics where possible, identify and discuss the environment, attributes, and best practices that characterize an effective CIO organization.
• OPM ECQ 1	1.1 LO 6: Compare an IT strategic plan with an overarching agency plan and determine performance gaps. (See also 5.1 LO 4 and 5.1 LO 6.)

Competency 1.2 - Governing laws and authorities • 5 U.S.C. 552 and 552a • 6 U.S.C. 485 • 29 U.S.C. 794d • Chapters 31, 35 and 36 of Title 44, U.S.C. • 40 U.S.C. Subtitle III • E-Government Act • GPRA Modernization Act of 2010 • EO 13231 • EO 13526 • EO 13556 • EO 13576 • OMB Circular A-11 • OMB Circular A-123 • OMB Circular A-130 • HSPD 7 • HSPD 12 • OPM ECQ 1	1.2 LO 1: Identify current and emerging legislation, regulations, and policies relevant to the CIO's responsibilities. Assess their provisions, including performance mandates, and discuss their organizational implications. (See also 5.1 LO 1.)
• OPM ECQ 1, 5	1.2 LO 2: Discuss how regulatory, oversight, and interagency policy groups impact a CIO's responsibilities and organization.
• ISO 38500 • ISO/IEC 27000 series • OPM ECQ 5	1.2 LO 3: Discuss the importance of standards issued by organizations such as the National Institute of Standards and Technology (NIST); the American National Standards Institute (ANSI); and the International Organization for Standardization (ISO) and their impact on the IT business environment.
	1.2 LO 4: Discuss the applicability of governing laws and authorities to contractor-managed/hosted systems and/or websites.
	1.2 LO 5: Discuss IT capability to track, evaluate and communicate emerging legislation, regulations, and intergovernmental legislation, including changes in acquisition regulations/guidelines.

Competency 1.3 - Federal government decision and policy-making processes • OMB Circular A-11 • OPM ECQ 1	1.3 LO 1: Discuss the IT strategic planning process. Identify internal and external drivers; organizational strengths, weaknesses, and culture; and future trends.
• OPM ECQ 1	1.3 LO 2: Apply a strategic planning process that crosswalks IT/CIO, enterprise-wide, and government-wide strategies, strategic goals, and performance objectives.
• OPM ECQ 1	1.3 LO 3: Discuss the advantages and limitations of different decision-making approaches. (See also 2.1 LO 11.)
• OPM ECQ 1	1.3 LO 4: Describe approaches needed to develop a supportive climate for IT innovation and provide examples of successful applications in government.
• OPM ECQ 1	1.3 LO 5: Identify evaluation methods and metrics to assess the CIO's effectiveness in supporting an agency's strategic plan.
Competency 1.4 - Linkages and interrelationships between Agency heads and their Chief Executive Officers	1.4 LO 1: Describe the roles of the Agency head, the various Chief Executive Officers (CXOs), and their interrelationships.
	1.4 LO 2: Discuss and analyze organizational structure and interaction, line and staff responsibilities, the flow of communications, independent and interdependent decision-making, and the contribution of IT and the CIO to the organizational structure, using a systems perspective. (See also 1.1 LO 4.)
	1.4 LO 3: Map the structure and the information flows of a CIO organization.

Competency 1.5 - Intergovernmental programs, policies, and processes	1.5 LO 1: Discuss the legislative, regulatory and coordination dimensions and mechanisms of intergovernmental programs, policies and processes. (Also see Competency 7.5.)
• 6 U.S.C. 485 • EO 13388 • PPD-1 • OMB M-11-02 • OPM ECQ 5 • U.S. Intelligence Community, Information Sharing Policy • National Strategy for Information Sharing: Success and Challenges in Improving Terrorism-Related Information Sharing	1.5 LO 2: Analyze the role of the CIO and the challenges associated with implementing effective internal and external agency information sharing. Include an examination of the laws, regulations and policies; technical issues; procedural obstacles; and cultural barriers. (Also see 3.5 LO 1 and 10.4 LO 2.)
• OPM ECQ 5	1.5 LO 3: Analyze government partnership opportunities enabled by technology that can assist the CIO in achieving mission requirements.
• Federal Advisory Committee Act • OMB Circular A-135 • OPM ECQ 5	1.5 LO 4: Discuss how government-wide policy groups and advisory groups impact agency operations.
• OPM ECQ 5	1.5 LO 5: Discuss the significance of management oversight, both internal and external (e.g., Congress, the Office of Management and Budget (OMB), the General Accountability Office (GAO), and the Office of the Inspector General (OIG)), and effective methods to create an open, ongoing dialogue between these entities and the CIO organization.
Competency 1.6 - IT governance • 44 U.S.C. 3603 • OMB M-09-02 • OMB M-11-29 • Federal CIO Council Charter • ISO 38500	*General Discussion: IT is an integral part of agency's overall governance and consists of the leadership and organizational structures and processes that ensure that the agency's IT sustains and extends the agency's mission by supporting its information management and delivery needs. CIOs not only must be a part of the overall agency governance, but also must ensure that they have functioning governance mechanisms for policy making, enforcement and decision making on IT issues that are effective, transparent, and accountable.*

	1.6 LO 1: Review the overall agency governance structure to determine where the CIO participates and with what kind of authority.
	1.6 LO 2: Identify where the CIO derives his/her authority – statutorily directed or by delegation – to participate in the agency's major decision making processes – namely, budgeting, requirements development, and acquisition.
	1.6 LO 3: Discuss the advantages and disadvantages of the CIO's role on various agency governance bodies.
	1.6 LO 4: Discuss the role of CIOs in other agencies' governance structures.

2.0: Leadership and Human Capital Management	*General Discussion: Management concepts are important <u>but</u> CIOs must move beyond management to leadership. This includes oversight over the individuals within their organization, and working to attract, retain, and develop their personnel.*
Competency 2.1 - Key CIO leadership attributes • OMB M-09-02 • OMB M-11-29 • OPM ECQs 1-5	2.1 LO 1: Compare the various roles and skills of a CIO with the Office of Personnel Management's listing of Executive Core Qualifications that all CIOs are expected to demonstrate.
	2.1 LO 2: Discuss the importance of CIOs identifying their own interpersonal skill sets, as well as those of their staff.
	2.1 LO 3: Compare and contrast different leadership styles and how effective they are in a CIO organization.
• OPM ECQ 1	2.1 LO 4: Discuss the relationship between program visionary leadership and technical visionary leadership and the need for both.
	2.1 LO 5: Define the communication process, and give examples of effective communication skills.
	2.1 LO 6: Identify and demonstrate behaviors related to effective listening and feedback.
	2.1 LO 7: Discuss barriers to communications in an interconnected world, and approaches to overcome and/or manage them.
	2.1 LO 8: Describe the range and effect of interpersonal communications (including media) in individual, small group, and organizational communication.
	2.1 LO 9: Discuss and demonstrate the application of the principles of individual behavior and group behavior in organizations.
	2.1 LO 10: Evaluate both need-based theories of motivation and process-based theories. Illustrate how to apply these theories in the workplace.
	2.1 LO 11: Discuss the advantages and limitations of different decision-making approaches, and identify methods of effective decision-making that support the specific agency mission of the CIO. (See also 1.3 LO 3.)
• OPM ECQ 2	2.1 LO 12: Describe the role of conflict in an organization and demonstrate effective conflict management skills.
• OPM ECQ 3	2.1 LO 13: Design approaches to champion initiatives.

Competency 2.2 - Professional development and career planning • 40 U.S.C. 11315 • 44 U.S.C. 3506 • OMB Circular A-130 • OPM ECQ 2	2.2 LO 1: Discuss the role of the CIO in creating and maintaining a supportive infrastructure for staff personal and professional development. Include in the discussion the responsibilities of managers and supervisors.
• OPM ECQ 2	2.2 LO 2: Identify approaches to maintain continuous learning to support mission critical competencies.
• OPM ECQ 2	2.2 LO 3: Discuss how to build a training program that recognizes and accommodates different learning styles.
• OPM ECQ 2	2.2 LO 4: Discuss different workforce organizational developmental tools, including the use of gap analysis. (See also 3.0 LO 1.)
• OPM ECQ 2, 4	2.2 LO 5: Analyze a variety of methods to establish IT career development paths and programs in government.
• OPM ECQ 2, 4	2.2 LO 6: Discuss the effectiveness of various staff recruitment, development and retention plans. (Also see Competency 2.6 on Attracting and retaining personnel.)
• OPM ECQ 4	2.2 LO 7: Discuss how to conduct succession planning in an organization.
• OPM ECQ 2, 4	2.2 LO 8: Discuss how to integrate generational differences in workforce planning and professional development programs.
Competency 2.3 - Competency performance and management	2.3 LO 1: Describe how IT certifications, testing, and academic degrees are used to build competency strength in the Federal Government.
	2.3 LO 2: Discuss how to create position descriptions and competency selection criteria that align to your agency's organizational design.
	2.3 LO 3: Identify and discuss positions, particularly those impacting IT, for which there are legislated or regulated competency requirements (e.g., IT acquisition, cybersecurity/IA, IT program/project management).
	2.3 LO 4: Compare and contrast methods to evaluate competency performance.
Competency 2.4 - Partnerships and team-building • OPM ECQ 2	2.4 LO 1: Discuss Organizational Development techniques and their role in team building and partnering. (See also 3.1 LO 1.)
• OPM ECQ 2	2.4 LO 2: Discuss the principles of group dynamics and how

	they can assist a manager in anticipating behavior.
• OPM ECQ 2	2.4 LO 3: List and define typical integrated project team roles.
• OPM ECQ 2	2.4 LO 4: Describe the team-building process, including the need for trust and the importance of empowerment.
• OPM ECQ 2	2.4 LO 5: Discuss and apply the principles of team leadership in a variety of settings including a matrix environment, an inter-organizational environment, and a systems environment.
• OPM ECQ 2	2.4 LO 6: Evaluate the contributions that self-awareness tools bring to team-building.
• OPM ECQ 2	2.4 LO 7: Discuss the dynamics of managing a team when alternative work sites and flexible work schedules are employed within the organization.
• OPM ECQ 2	2.4 LO 8: Discuss the challenges of vendor integration into team projects. (See also 6.8 LO 3.)
• OPM ECQ 2	2.4 LO 9: Identify appropriate team-building approaches to be used in multi-disciplinary, inter-organizational, and partnership situations.
• OPM ECQ 5	2.4 LO 10: Describe the technical and cultural challenges of cross-boundary and interagency partnering. (See also Competency 3.5 on Cross-boundary collaboration.)
Competency 2.5 - Personnel performance management • OPM ECQ 4	2.5 LO 1: Evaluate advantages and disadvantages of different performance management and appraisal approaches.
• OPM ECQ 4	2.5 LO 2: Discuss proven methods of communicating job expectations.
• OPM ECQ 4	2.5 LO 3: Discuss how to engage staff members in establishing their performance objectives.
• OPM ECQ 4	2.5 LO 4: Justify the value of timely performance feedback, and generational perspectives on desired frequency.
• OPM ECQ 3	2.5 LO 5: Describe the role of accountability in creating a results-driven organization.
• OPM ECQ 4	2.5 LO 6: Discuss how the implementation of Competency 2.5, learning objectives 1 through 5, prepares managers to effectively address poor performance.

Competency 2.6 – Attracting, motivating, and retaining IT personnel • OPM ECQ 4	2.6 LO 1: Discuss the role that encouragement, empowerment, recognition and frequent performance feedback play in employee engagement and retention. (See also 2.2 LO 6.)
• OPM ECQ 2, 4	2.6 LO 2: Describe the ways in which a culture of trust functions as a motivator, encourages innovation, and retains personnel.
• OPM ECQ 2	2.6 LO 3: Design approaches to develop and implement a culture of trust.
• OPM ECQ 2	2.6 LO 4: Discuss the opportunities and challenges present in a workplace that exhibits diversity of all kinds, including, but not limited to, gender, race, creed, sexual orientation, national origin and generational differences.
• OPM ECQ 4	2.6 LO 5: Describe how a clearly defined and jointly held vision improves personnel recruiting, retention and performance.
• OPM ECQ 4	2.6 LO 6: Discuss the importance of professional development opportunities and career management support in creating an attractive work environment for potential and current employees.
	2.6 LO 7: Explain how lack of resources can impact job satisfaction, employee engagement and the achievement of organizational mission.
• OPM ECQ 2, 4	2.6 LO 8: Review best practices for acquiring, developing and retaining high caliber, multi-generational IT professionals.

3.0: Process and Change Management	*General Discussion: The paramount role of the CIO is as Chief Visionary of the organization's information and technology—critical enablers for achieving mission and improving efficiency. Change management encompasses far more than a single leader's perspective. The CIO works in strong partnership with the CXOs and other key stakeholders as part of the change management process. Open, effective communications are essential to ensure organizational buy-in.*
• OPM ECQ 1	3.0 LO 1: CIOs frequently must lead change (technology adoption, skill transfer, etc.) in an organization. Discuss the concept of change, and the dimensions of behavioral change. (See also 2.2 LO 4 and 2.4 LO 1.)
• OPM ECQ 1	3.0 LO 2: Discuss the role of leadership, including that of the CIO, in successful change initiatives.
• OPM ECQ 1, 3	3.0 LO 3: Justify the importance of stakeholder "buy-in" in successful change efforts.
	3.0 LO 4: Identify and demonstrate approaches a CIO can use to achieve stakeholder support in change efforts.
	3.0 LO 5: Federal CIOs work within a large system that includes the Office of Management and Budget, the Federal CIO Council, and different administrations, executing multiple initiatives that continuously require changes. Discuss the dimensions of the government environment as a factor in successful change management.
Competency 3.1 - Organizational Development	*General Discussion: It is important that CIOs be familiar with Organizational Development (OD) concepts and OD's importance as an independent discipline. CIOs need to be able to critically assess the organization against strategic goals, be familiar with the tenets of change management, and assess planned change from a systems perspective*.
	3.1 LO 1: Discuss the concepts and methods of Organizational Development. (See also 2.4 LO 1.)
• OPM ECQ 1	3.1 LO 2: Discuss organizational assessment methods and metrics used to assess the need for change.
• OPM ECQ 1	3.1 LO 3: Describe various change techniques and tools.
• OPM ECQ 1	3.1 LO 4: Design approaches (including the identification of key influential individuals) to prepare the workplace for change.
• OPM ECQ 1	3.1 LO 5: Discuss organizational resistance to change, including the identification of barriers and strategies for overcoming resistance.

• OPM ECQ 1	3.1 LO 6: Differentiate between voluntary and mandated change strategies and the approaches to their implementation.
• OPM ECQ 1	3.1 LO 7: Design a comprehensive plan to implement, communicate, and champion an organizational change initiative.
Competency 3.2 - Process management and control	3.2 LO 1: Discuss the principles of process management and control.
	3.2 LO 2: Compare, contrast and evaluate the major tools, techniques and methods of process management.
	3.2 LO 3: Describe gap analysis and how to apply its results within an organization.
	3.2 LO 4: Evaluate the importance of internal control systems within the CIO organization.
Competency 3.3 - Quality improvement models and methods	3.3 LO 1: Explain the different uses and meanings of the term “quality.”
	3.3 LO 2: Assess and prioritize quality factors used in business, information and technical areas.
	3.3 LO 3: Discuss the dimensions of quality when addressing customer, employee and stakeholder expectations.
• OPM ECQ 3	3.3 LO 4: Discuss how quality can be integrated into the culture of the organization.
	3.3 LO 5: Discuss how to integrate quality dimensions into strategic planning, performance goals and objectives.
• OPM ECQ 3	3.3 LO 6: Describe the CIO's responsibilities regarding quality improvement.
	3.3 LO 7: Compare and contrast programs and standards associated with quality management. Include in the discussion ISO 9001 and 20000, the Baldrige Award, Quality Function Deployment (QFD), Capability Maturity Model Integration (CMMI), and the Information Technology Infrastructure Library (ITIL).
Competency 3.4 - Business process redesign/reengineering models and methods	3.4 LO 1: Define Business Process Improvement, redesign, and reengineering (BPI/BPR).
	3.4 LO 2: Trace and assess the history, evolution, and relationships of Business Process Reengineering (BPR), Business Process Improvement (BPI), and other business process transformation initiatives.
	3.4 LO 3: Discuss examples of successful BPI, redesign, and BPR initiatives within government.

	3.4 LO 4: Discuss the models and methods that may be used in a comprehensive BPI effort. Include discussion of continuous process improvement tools and evaluate their benefits.
	3.4 LO 5: Discuss the unique challenges associated with undertaking business process re-design.
	3.4 LO 6: Identify the key management actions required to manage a portfolio of process improvement initiatives across the enterprise.
	3.4 LO 7: Design an integrated management approach to support embedding and institutionalization of process changes in organizations.
Competency 3.5 - Cross-boundary process collaboration • OPM ECQ 5	3.5 LO 1: Discuss inter-agency, industry and academic collaboration initiatives and best practices, including common process languages, collaborative technology interfaces and common process standards. (See also 1.5 LO 2 and 2.4 LO 10.)
• OPM ECQ 5	3.5 LO 2: Identify cultural challenges a CIO may face in cross-boundary, inter-agency collaborations.
• OPM ECQ 5	3.5 LO 3: Examine business cases that highlight the successes and failures of inter-agency collaboration efforts.

4.0: Information Resources Strategy and Planning	*General Discussion: IT must be a value-adding dimension of the business plan. Information Resources Management (IRM) strategic planning must begin with the business strategic planning process and integrate with the organization's business functions and plans since business planning and IRM planning are parallel and coupled processes. IRM planning should also address cross-governmental and inter-agency planning issues as well as external drivers.*
• OPM ECQ 1	4.0 LO 1: Describe the principles of strategic planning as they apply to IT.
	4.0 LO 2: Describe the relationship between IT strategic planning and IT functional analysis.
• OPM ECQ 1	4.0 LO 3: Describe how IT visionary strategic planning is linked to enterprise/program visionary strategic planning.
Competency 4.1 - IRM baseline assessment analysis	4.1 LO 1: Define and describe performance goals and distinguish performance goals from performance standards.
	4.1 LO 2: Discuss benchmarking, particularly as applied to IT hardware, software, networking (e.g., protocols) and IT staff skills and abilities.
	4.1 LO 3: Evaluate a current baseline analysis against established benchmarks.
	4.1 LO 4: Describe the ways in which benchmarks may be used to forecast performance.
	4.1 LO 5: Explain the importance of IT performance assessment and analysis, and summarize how results can be used to develop IRM strategies and plans that support mission objectives and business goals.
	4.1 LO 6: Design performance analysis and assessment approaches that address each element of an IT organization.
	4.1 LO 7: Discuss the baseline review and the development of total cost of ownership estimates. Include correlation to enterprise architecture, capital planning and investment and systems development lifecycle.
Competency 4.2 - Interdepartmental, inter-agency IT functional analysis	4.2 LO 1: Define functional analysis in an IRM setting.
	4.2 LO 2: Define the purpose and goals of IT functional analysis. Discuss when cross-functional work is desirable and when it is not desirable.
	4.2 LO 3: Using a mission statement and baseline analysis, analyze the functional and cross-functional requirements for an IT group.

	4.2 LO 4: Using an example of an interagency IT partnership, assess the potential challenges resulting from scope expansion.
	4.2 LO 5: List and describe functional analysis issues (e.g., security, privacy, accessibility, and open access). (See also 9.2 LO 1.)
	4.2 LO 6: Compare and contrast various potential solutions to IT needs, including, "Use what we've got. Build new. Acquire from the private sector. Acquire from the public sector," etc.
	4.2 LO 7: Discuss the statement that "cross-functional IT aspects must be embedded in the system." Include the communication channels (interdepartmental, interagency, and intergovernmental) appropriate to the level of discussion.
Competency 4.3 - IT planning methodologies	4.3 LO 1: List and describe a comprehensive IT planning process.
	4.3 LO 2: Compare and contrast the range of IT planning methodologies, including gap analysis, weighted priorities, modeling techniques, Capability Maturity Modeling, Business Process Improvement and Business Process Reengineering.
Competency 4.4 - Contingency and continuity of operations planning (COOP) • NSPD-51/HSPD-20 • NCSD 3-10 • FCD 1 and 2 • OMB Circular A-130, Appendix III • NIST SP 800-34	4.4 LO 1: Discuss the need for contingency plans to protect against costly IT events caused by manmade activities and natural disasters; include discussion of potential risks and how to prioritize them.

	4.4 LO 2: Discuss the challenges of garnering the needed resources to protect against costly IT events.
	4.4 LO 3: Discuss the value of interoperability of resources in support of contingency needs.
	4.4 LO 4: Discuss the benefits of periodically reviewing IT contingency plans.
	4.4 LO 5: Develop a mock COOP with policies, procedures, plans and annual testing and reporting requirements to ensure the continuity of operations for an agency's information systems.
	4.4 LO 6: Evaluate (test) a plan to ensure the continuity of operations for information systems that support the operations and assets of an agency.
Competency 4.5 - Monitoring and evaluation methods and techniques	4.5 LO 1: Describe methods to assess the value, benefit and cost of IT and its impact on the organization.
	4.5 LO 2: Discuss the value of Activity Based Costing (ABC) in demonstrating the value and benefits of IT.
	4.5 LO 3: Describe and evaluate the applicability of frameworks such as Capability Maturity Model Integration (CMMI), ISO 9001, the Information Technology Infrastructure Library (ITIL) and Control Objective over Information and Related Technology (COBIT).
	4.5 LO 4: Describe and evaluate the strengths and weaknesses of qualitative and quantitative data collection techniques including interviews, elite interviews, focus groups, surveys, questionnaires, etc. Include discussion of reliability and validity of survey data.
	4.5 LO 5: Discuss the use of questionnaires and other survey instruments for operational analysis, addressing customer satisfaction and identifying qualitative gaps that may exist in IT services. (See also 5.6 LO 3.)

5.0: IT Performance Assessment: Models and Methods	*General Discussion: The CIO has the challenge of meeting both customer and organizational needs established in the agency's business plan. In order to ensure those needs are being met, the CIO must understand the importance of the qualitative and quantitative baseline assessment measures and their use in the performance assessment cycle.*
Competency 5.1 - Government Performance and Results Act (GPRA) and IT • 5 U.S.C. 552 and 552a • 29 U.S.C. 794d (Section 508 of the Rehabilitation Act of 1973, as amended) • Subtitle III of Title 40, U.S.C. • Chapters 31, 35 and 36 of Title 44, U.S.C. • Chapter 9 of Title 31, U.S.C. (Chief Financial Officers Act of 1990) • E-Government Act • GPRA Modernization Act of 2010 • Presidential Memo, Transparency and Open Government • EO 13576 • OMB M-09-12 • OMB M-11-17 • OMB M-11-29 • OMB, 25 Point Implementation Plan to Reform Federal Information Technology Management	5.1 LO 1: List current federal performance legislation and describe/discuss the performance mandates that a CIO must address. (See also 1.2 LO 1.)
	5.1 LO 2: List and describe qualitative contributions to business value including usability, accessibility, efficiency, productivity and perceived value.
• OMB M-11-26 • OMB M-12-10 • OMB M-12-20 • OMB Circular A-11	5.1 LO 3: Illustrate sources of data that can be used to support performance assessment conclusions and decisions.
• OPM ECQ 1	5.1 LO 4: Describe how IT strategic planning relates to the business mission, vision, strategy, goals and objectives of an organization. (See 1.1 LO 6.)
• OPM ECQ 1	5.1 LO 5: Describe how IT initiatives support the goals within an IT strategic plan.
• OPM ECQ 1	5.1 LO 6: Develop an IT strategic plan that is integrated with

	organization mission objectives, business goals, and target architecture. (See 1.1 LO 6 and 11.3 LO 6.)
• OPM ECQ 3	5.1 LO 7: Determine how best to identify key external and internal IT stakeholders and customers and how to interface with each for optimum results.
Competency 5.2 - System development decision making	5.2 LO 1: Identify criteria to be used when analyzing whether to replace an existing system.
	5.2 LO 2: Describe best practices for identification and documentation of stakeholder requirements related to the development of a potential new system.
	5.2 LO 3: Compare and contrast the characteristics and the challenges involved in "new" systems, both those that are replacing existing systems, and those that are completely new.
	5.2 LO 4: Identify criteria and integrate "go/no go" checkpoints into a development lifecycle.
	5.2 LO 5: List and describe the decision tools and evaluation systems that are typically used to make go/no go decisions.
	5.2 LO 6: Identify and evaluate the criteria required to determine whether to "stop" or "kill" a project.
Competency 5.3 - Measuring IT success	5.3 LO 1: List and explain criteria used to determine IT success in meeting stakeholder needs, customer needs and mission performance.
	5.3 LO 2: Define the terms measure, milestone, metric and objective and their functions in measuring success.
	5.3 LO 3: Describe the differences between leading and lagging indicators and give examples of both.
	5.3 LO 4: Discuss the need for measurements, the limits of analysis, and the hazards of measurement for measurement's sake.
	5.3 LO 5: Distinguish between outcome (what the system needs to achieve) and output (what the system does) in defining performance measures.
	5.3 LO 6: Discuss the importance of identifying a few critical measures of IT success, and how to keep them visible.
	5.3 LO 7: Demonstrate the value of continuous assessment of IT strategic plan milestones.

Competency 5.4 - Defining and selecting effective performance measures	5.4 LO 1: List, describe, and evaluate techniques that are appropriate for measuring effective performance. Identify where these techniques may be found. Include in the discussion the Goals, Questions, Metrics, Measures (GQMM) approach, the Balanced Scorecard, Benchmarking, Best Practices, and OMB Circular A-11.
• OPM ECQ 3 • OMB M-11-26 • OMB M-12-10 • OMB M-12-20 • OMB Circular A-11 • OMB Guidance on Exhibit 300	5.4 LO 2: Describe how to choose performance measures that align with stakeholder needs, mission, vision, critical success factors, etc.
• OPM ECQ 3	5.4 LO 3: Discuss the advantages and disadvantages of building user feedback into the design and development of performance measures.
Competency 5.5 - Evaluating system performance • OMB M-11-26 • OMB M-12-10 • OMB Circular A-11 • OMB Guidance on Exhibit 300	5.5 LO 1: Identify, evaluate and report on sources of performance evaluation information including internal databases, government-wide databases, proprietary databases, and available web sites.
	5.5 LO 2: Discuss how to evaluate whether technology is fulfilling strategic mission objectives and business needs as well as the tactical dimensions of service, information and system quality.
• OPM ECQ 3	5.5 LO 3: Discuss the approaches to, and the value of, identifying and prioritizing customers and stakeholders.
Competency 5.6 - Managing IT reviews and oversight processes • OMB M-11-26 • OMB M-12-10 • OMB M-12-20 • OMB Circular A-11 • OMB Guidance on Exhibit 300	5.6 LO 1: Discuss the significance and impact of both internal and government-mandated IT reviews.
	5.6 LO 2: Define the roles and responsibilities of managers (program managers, project managers, program leads, etc.) in the IT review process.
	5.6 LO 3: Identify key performance parameters for each phase in the lifecycle, using a specified project plan. (See also

	4.5 LO 4.)
	5.6 LO 4: Design a method to ensure that data collected in the assessment process is used in the review and decision making processes.

6.0: IT Project and Program Management	*General Discussion: The relationship between project management and program management is interdependent, not discrete, and progressively cumulative. A project is a specific investment having defined goals, objectives, requirements, lifecycle cost, a beginning and an end that delivers a specific product, service or result. A program is typically a group of related work efforts, including projects, managed in a coordinated way. Programs usually include elements of ongoing work. For program management processes to be mature, project management processes must be mature. IT Program Managers should be skilled in both IT Project and IT Program Management Competencies*
• ANSI/PMI 99-001-2008 • Project Management Book of Knowledge	6.0 LO 1: Describe the elements included in the project management lifecycle, including initiation, planning, execution, controlling and monitoring, and closing.
	6.0 LO 2: Discuss the CIO's lifecycle responsibility for IT project and program management.
	6.0 LO 3: Examine the importance of ethics, integrity, objectivity and accountability in IT project and program management.
• ANSI/PMI 99-001-2008	6.0 LO 4: Explore sources of project management standards.
• OMB M-04-19 • OMB M-11-29 • OMB Guidance on Exhibit 53 • OMB Guidance on Exhibit 300 • OFPP Policy Memo on FAC-P/PM dtd April 25, 2007	6.0 LO 5: Examine federal IT project and program manager qualification requirements and their impact on agency operations.
Competency 6.1 - Project scope and requirements management	6.1 LO 1: Using a case study, analyze the business or mission needs that are driving project requirements.
	6.1 LO 2: List and define the elements involved in the scope (money, time, people, impact, etc.) of a specified project or program being considered.
	6.1 LO 3: Discuss the ways in which project requirements affect project scope and scope management.
	6.1 LO 4: Discuss how the project or program scope elements link to organizational mission and goals.
	6.1 LO 5: Assess potential positive and negative effects that arise from change (mission, organizational structure, organizational resources, etc.).
	6.1 LO 6: Discuss and design approaches to both track and control project requirements, technology changes, and user

	needs changes.
• NIST SP 800-128	6.1 LO 7: Discuss approaches to configuration management and develop procedures for establishing and maintaining a Configuration Control Board (CCB). (See also 9.6 LO 4.)
	6.1 LO 8: Illustrate how poor requirements management may cause scope creep.
	6.1 LO 9: Evaluate the decision-making methods and tools (both macro and micro) and analyze the outputs they make available to the project/program manager.
	6.1 LO 10: Discuss the implications of rapid design modeling techniques and methods on requirements and scope management. Include discussion on use of pilots and prototypes.
	6.1 LO 11: Describe the relevant functional requirements contained in DoD 5015.2-STD, “Design Criteria for Electronic Records Management Software Applications” and discuss their impact on system design and implementation.
Competency 6.2 - Project integration management	6.2 LO 1: Define and illustrate project integration and implementation.
	6.2 LO 2: Develop plans to integrate project management and business management.
	6.2 LO 3: Establish software management approaches to include promotion of process improvements, commercial off-the-shelf (COTS) risk assessment, human systems integration design and applications security analysis.
	6.2 LO 4: Discuss and give examples of the importance of innovation and creative thinking in creating alternate program integration strategies.
	6.2 LO 5: Describe integration across programs including the reallocation of resources.
	6.2 LO 6: Compare, contrast and evaluate available Knowledge Management tools.
	6.2 LO 7: Assess the value of electronic communication tools as an integration driver.
Competency 6.3 - Project time, cost, and performance management	6.3 LO 1: Discuss concepts of project planning, such as Work Breakdown Structure (WBS) development and critical path analysis and their relationship to project delivery.
• OMB M-10-27 • GAO-09-3SP	6.3 LO 2: Describe and evaluate project management planning techniques and tools that support the project lifecycle.
	6.3 LO 3: Describe and evaluate concepts of IT baseline

	management for project planning and performance measurement. Describe the relationship of processes, such as Earned Value Management, operational analysis, and business performance measurement, to IT baseline management.
	6.3 LO 4: Identify and evaluate metrics to manage cost, schedule, and performance throughout the project lifecycle.
	6.3 LO 5: Using a business case and the federal Techstat model, analyze project performance, resource usage, and cost and schedule management. Discuss the potential tradeoffs required to balance competing drivers.
• OMB M-10-27 • OMB Guidance on Exhibit 300 • ANSI/EIA 748	6.3 LO 6: Discuss the required use of Earned Value Management by OMB to evaluate the performance of major federal IT investments.
	6.3 LO 7: Use an Earned Value Management System to analyze a business case.
	6.3 LO 8: Discuss the importance of program control processes and industry best practices.
	6.3 LO 9: Discuss the importance of financial management techniques and tools.
Competency 6.4 - Project quality management	6.4 LO 1: Define characteristics of quality; include usability, quality assurance and quality control. (See also Competency 3.4 on Quality improvement models and methods.)
	6.4 LO 2: Identify quality requirements and establish evaluation metrics to achieve those requirements.
	6.4 LO 3: Identify and discuss ways to build quality into systems.
	6.4 LO 4: Design and implement approaches to obtain feedback from users.
	6.4 LO 5: Discuss the advantages of independent verification and validation (IV&V) and design approaches to tie IV&V to the quality assurance program.
Competency 6.5 - Project risk management	6.5 LO 1: Define risk. (See also 7.2 LO 1.)
	6.5 LO 2: Define the risk management process.
• ISO 31000 series	6.5 LO 3: Discuss technical, cost, supply chain, and management capability risks associated with project management. (See also 7.3 LO 2.)
• DoD Acquisition Risk Management Guide, 6th Edition, Version 1.0	6.5 LO 4: Discuss the use of risk management tools, including a risk register.

• SEI at Carnegie Mellon University	
	6.5 LO 5: Demonstrate the ability to perform SWOT (Strengths, Weaknesses, Opportunities and Threats) analysis.
	6.5 LO 6: Identify approaches to quantify risk assessment and to prioritize among risks.
	6.5 LO 7: Describe and evaluate the risk mitigation process, and how it is tailored to particular situations.
	6.5 LO 8: Evaluate monitoring and control systems and discuss their implementation.
	6.5 LO 9: Discuss the need for continuous risk monitoring throughout the project or program lifecycle.
	6.5 LO 10: Describe budget strategies to mitigate the impact of changes in project scope.
Competency 6.6 - System lifecycle management	6.6 LO 1: Discuss the IT lifecycle as a discipline. List and describe the components of the system lifecycle.
• SEI at Carnegie Mellon University • ISO/IEC 12207 • ISO 9000 series	6.6 LO 2: List and describe the standards that apply to the lifecycle.
	6.6 LO 3: Identify the impacts of costs, benefits, risks, resources, and time to market on the system lifecycle.
	6.6 LO 4: Distinguish between system development lifecycle and the system lifecycle.
	6.6 LO 5: Define and construct various project documents required throughout the system lifecycle and discuss how often they should be updated.
	6.6 LO 6: Describe the impact of Commercial-off-the-shelf (COTS) availability to the build or buy decision.
	6.6 LO 7: Discuss the heuristics of lifecycle—when to know when you have enough, etc. Include Total Cost of Ownership, lessons learned, etc.
	6.6 LO 8: Discuss the importance of managing change.
.	6.6 LO 9: Discuss the complexities associated with the closeout of systems, including end of life, the termination of systems, destruction of databases, etc.
	6.6 LO 10: Discuss strategies to increase investment effectiveness, such as agile, incremental development.

Competency 6.7 - Software development, testing, and implementation • ISO 9000 series • ISO/IEC 12207	6.7 LO 1: Evaluate the strengths and weaknesses of different models, approaches and methodologies relating to software development such as CMMI, Rapid Application Development (RAD), Joint Application Design (JAD), Object-Oriented (OO) software, Spiral Development, agile development, and emerging best practices. (See also Competency 12.6 on Software development technology.)
	6.7 LO 2: Discuss the importance of adopting and applying a systems engineering perspective and process to software development.
	6.7 LO 3: Develop an analytical process to support the make versus buy decision.
	6.7 LO 4: Discuss Pareto's 80/20 law as it applies to software development.
	6.7 LO 5: Discuss federal requirements for privacy, security, records management and accessibility in relation to software development. (See also 8.5 LO 5 and 9.2 LO 1.)
• ISO/IEC 9126	6.7 LO 6: Describe elements for evaluating software quality and how they would be applicable in testing software capabilities. (See also 8.5 LO 5.)
	6.7 LO 7: Discuss available tools, techniques, and metrics for software testing.
Competency 6.8 - Vendor management	6.8 LO 1: Discuss how to craft service level agreements which support mission and business objectives.
	6.8 LO 2: Discuss best practices for vendor selection criteria and processes.
	6.8 LO 3: Discuss how to establish useful vendor management policies and conformance criteria. (See also 2.4 LO 8.)
	6.8 LO 4: Discuss how to implement vendor management techniques that support long term business value and resource management.
	6.8 LO 5: Discuss the importance of vendor exit strategies in order to minimize disruption to IT services.
Competency 6.9 - IT program management leadership	6.9 LO 1: Discuss the characteristics of highly effective IT program managers.
	6.9 LO 2: Examine practices to influence and manage a broad set of stakeholder communities engaged in an IT program.
	6.9 LO 3: Examine ways IT leaders use methods of effective conflict management and negotiation.
	6.9 LO 4: Identify and discuss the steps required to

	successfully steward an integrated project team.
	6.9 LO 5: Design governance model processes for IT program management oversight and decision making.
	6.9 LO 6: Describe the role of vendors as strategic partners in IT programs.

7.0: Capital Planning and Investment Control (CPIC) • Title V, Acquisition Management, Federal Acquisition Streamlining Act of 1994, PL 103-355) • 31 U.S.C. Chapter 9 • Subtitle III, Title 40 U.S.C. • OMB Circular A-11 • OMB Circular A-94 • OMB Circular A-123 • OMB Circular A-127 • OMB Circular A-130 • OMB M-10-27 • OMB M-11-29 • NIST SP 800-65	*General Discussion: It is essential that CIOs understand the importance of Capital Planning and Investment Analysis. Capital planning is needed to provide a framework for running government with the same disciplines as private business. In addition to passage of the Clinger-Cohen Act (now codified in Title 40), there is an array of other legislation and fiscal guidance which are significant to effective Capital Planning and Investment Control.*
• Statutory Pay-As-You-Go Act of 2010	7.0 LO 1: Discuss the appropriation process and how politics (both local agendas and national issues) may affect the capital planning and investment control process.
• CMU/SEI-2002-TR-010, Software Acquisition Capability Maturity Model (SA-CMM)	7.0 LO 2: Schematize the entire IT lifecycle (using your agency or component's budgeting cycle or SEI's Software Acquisition Capability Maturity Model at Carnegie Mellon). Include both funding and retirement, and show how integral performance measures can support each phase of the cycle.
	7.0 LO 3: Discuss the importance of aligning capital planning with the agency mission.
	7.0 LO 4: Evaluate the roles that core mission, outsourcing and redesign play in CPIC.
Competency 7.1 - CPIC best practices	7.1 LO 1: Identify and evaluate current CPIC best practices.
	7.1 LO 2: Develop approaches to examine internal and external processes and practices and to develop appropriate benchmarks.
Competency 7.2 - Cost benefit, economic, and risk analysis • OMB Circular A-94 • OMB M-12-06 (or current memorandum on discount rates)	7.2 LO 1: Describe and interpret a variety of methodologies used in cost benefit, economic and risk analysis. (See also Competency 6.5 on Project risk management).
	7.2 LO 2: Prepare a set of cost benefit, economic and risk analysis methodologies that can provide common standards for use throughout a large organization. (See also 7.6 LO 4.)
	7.2 LO 3: Compare and contrast the implications of

	commonly used metrics such as ROI, NPV, Internal or Modified Internal Rate of Return (IRR, MIRR) etc. This comparison should address not only the outputs of the metrics, but also the assumptions upon which the metrics are based.
	7.2 LO 4: Identify and define processes to ensure the consistency of applied metrics across a range of projects under consideration in the capital planning process. (See also 7.8 LO 1.)
	7.2 LO 5: Analyze cost and economic data, assess its quality, and communicate its meaning to others.
	7.2 LO 6: Identify and evaluate qualitative approaches that can be used in risk analysis in addition to the more traditional quantitative methodologies.
	7.2 LO 7: Discuss the purpose for doing a risk-adjusted ROI as part of developing a solid business case for a major IT investment.
	7.2 LO 8: When presented with a business need, evaluate a variety of solutions that include, but are not limited to, IT-based solutions.
Competency 7.3 - Risk management models and methods • ISO 31000 series • NIST SP 800-37	7.3 LO 1: Discuss the reasons why risk analysis and risk management are vital. Include discussion of the role risk management plays and how the specifics relate to the organization and its mission.
	7.3 LO 2: Discuss and illustrate major areas of risk such as cost, schedule, performance, technical considerations (including obsolescence) and management capability. (See also 6.5 LO 3.)
	7.3 LO 3: Compare and contrast the commonly accepted standards, tools, and methods used in risk management.
• OMB Circular A-94 • OMB Guidance on Exhibit 300 • OMB M-12-06 (or current memorandum on discount rates)	7.3 LO 4: Evaluate and apply commonly used best practices risk management models.
	7.3 LO 5: Apply risk management models and methods to selected business cases.
	7.3 LO 6: Discuss the limitations of risk management models and areas of risk that may not be captured within a modeling scenario.

Competency 7.4 - Weighing benefits of alternative IT investments • OPM ECQ 3	7.4 LO 1: Develop an analysis and decision-making process to ensure that a CIO will evaluate all alternatives (and not only IT alternatives) for new requirements.
• OPM ECQ 3	7.4 LO 2: Compare and contrast the commonly accepted standards, tools, and methods available for evaluating benefits of alternative IT investments.
• OMB Circular A-11 • OMB Circular A-94 • OPM ECQ 3	7.4 LO 3: Compare and contrast the advantages of uniform IT investment assessment standards versus the value of flexibility in assessing alternative IT investments.
	7.4 LO 4: Identify and discuss examples of shared solutions between organizations to leverage investments.
• OMB Circular A-11 • OMB Circular A-94 • OPM ECQ 3	7.4 LO 5: Discuss the role of forecasting in cost-benefit analysis.
• OMB Circular A-94 • OPM ECQ 3	7.4 LO 6: Evaluate cost benefits of alternative IT-and non IT-solutions, and be able to support and justify the best alternative.
	7.4 LO 7: Identify the types of decision tools and criteria that are used within the development lifecycle to determine when a system has reached maturity.
Competency 7.5 - Capital investment analysis models and methods	7.5 LO 1: Compare, contrast and demonstrate the use of the various capital investment models and methods.
	7.5 LO 2: Analyze select IT capital investment business cases using appropriate analysis models.
	7.5 LO 3: Compare, contrast and demonstrate the use of the various investment assessment models and methods, including Balanced Scorecard, as well as discussion of federal TechStat reviews and IT Dashboard ratings of investments.
Competency 7.6 - Business case analysis	7.6 LO 1: Discuss the elements of a comprehensive business case analysis, including management, customers, and technical costs.
	7.6 LO 2: Using case studies, examine how business case analysis provides the means to evaluate the quantitative and qualitative aspects of competing investment opportunities.
	7.6 LO 3: Verify the validity of measurements used in developing/calculating investment metrics.
	7.6 LO 4: Compare and contrast the models and methods of business case analysis, both in government and in industry. (See also 7.2 LO 2.)

Competency 7.7 - Investment review process	7.7 LO 1: Discuss the need for an investment review process. Identify the types of information that are needed and discuss identities and roles of key decision-makers.
	7.7 LO 2: Identify the information and measurement tools that will be needed for the investment review process. Include "checkpoints" that may trigger additional information.
	7.7 LO 3: Discuss different approaches to the investment review process. Include approaches that are oriented to the culture of the specific organization (e.g., some organizations are detailed and quantitative, others are consensus-based), and how to select an appropriate approach based on organizational culture.
• OMB Circular A-11	7.7 LO 4: Describe the stages of an investment review process.
• OMB Guidance on Exhibit 300	7.7 LO 5: Describe the capital planning process in lifecycle terms. Include OMB Circular A-11 in the discussion.
Competency 7.8 - IT portfolio management • Subtitle III, Title 40 U.S.C. • OMB Circular A-130	7.8 LO 1: Discuss the steps required to move from assessment of individual IT capital investments to an integrated process for managing IT investments as portfolios. (See also 7.2 LO 4.)
	7.8 LO 2: Identify and discuss portfolio management categorization techniques.
	7.8 LO 3: Establish analysis criteria and a process to link portfolio objectives to an agency's vision, mission, goals, objectives and priorities.
	7.8 LO 4: Discuss strategies and methods to support portfolio tradeoff decision making.
• OMB M-12-10	7.8 LO 5: Examine how the process of balancing portfolios, by terminating or adding investments, effectively contributes to agency goal achievement.
• EO 13589 • OMB M-11-29 • OMB M-12-10	7.8 LO 6: Discuss Federal Government requirements and initiatives to eliminate waste and duplication within IT portfolios.

8.0: Acquisition • OMB M-11-29 • OMB 25 Point Plan • OMB, OFPP memo on Guidance for Specialized IT Acquisition Cadres	*General Discussion: Acquisition links technology investment to the business outcomes and results, as defined by the end consumer. Acquisition needs to move from what been a singular focus on process to one that considers both process and objectives. Acquisition anticipates what is needed before it is officially stated, and develops requirements that include the end users and must be linked to business outcomes.* *The CIO must understand the new dynamic, and understand lifecycle management. He/she must move from a risk-averse process to one of risk management, and create an innovative acquisition environment throughout the organization. The CIO should monitor changes in acquisition models and methods.* *Acquisition includes four stages–(1) Defining the business objective; (2) Requirements definition and approval; (3) Sourcing and (4) Post-Award management—which are each critical to a successful IT acquisition.*
	8.0 LO 1: Compare and contrast acquisition, contracting, and procurement.
	8.0 LO 2: Describe each phase of the acquisition lifecycle.
	8.0 LO 3: Describe the CIO's involvement in the early phases of acquisition management (i.e., concept exploration and development of requirements).
	8.0 LO 4: Discuss how to encourage ethical acquisition behavior for all involved in the acquisition process.
Competency 8.1 - Acquisition strategy	8.1 LO 1: Describe how the strategic plan, annual performance plan, enterprise architecture and capital planning process drive the acquisition strategy.
	8.1 LO 2: Demonstrate the development of an acquisition strategy. Include interpretation of internal and external environments, shared and cloud first strategies,the business, fiscal and political environments, awareness of A76 methodology, contracting strategy, and technological and environmental changes in the development of the acquisition strategy.
	8.1 LO 3: Identify and evaluate the range of alternatives to acquisition that should be explored in the pre-phase of the project. Include the roles of technology, reengineering, architecture, training, process improvement, procedure modification, elimination of functions, etc., in the listing of alternatives.
	8.1 LO 4: Discuss the differences between acquisition as a

	planned event and as a reactive event.
	8.1 LO 5: Illustrate the use of cost, schedule, technology, and performance goals in the planning and management of acquisitions.
	8.1 LO 6: Identify examples of issues that should be included in a project description and statement of work.
	8.1 LO 7: Identify the issues a project manager needs to address in a procurement management plan.
Competency 8.2 - Acquisition models and methodologies	8.2 LO 1: Compare, contrast, and evaluate various acquisition philosophies. Include, but do not limit the identification to: changing the operational process instead of purchasing; doing the work in house or outsourcing; outsourcing to one or to several contractors; intergovernmental outsourcing; unitary Requests for Proposal (RFP) or multiple awards; and the level at which the acquisition is managed.
	8.2 LO 2: Define the components typically included in an acquisition model. These components might include the relationship between government and supplier, internal relations, the motivation of the supplier, elements of sourcing, etc.
	8.2 LO 3: Discuss how to select an acquisition model that fits the organization's mission, needs, and culture.
	8.2 LO 4: Compare, contrast, and evaluate traditional and streamlined methodologies used for federal IT acquisition.
	8.2 LO 5: Discuss the acquisition implications from federal initiatives to increase inter-agency shared services.
	8.2 LO 6: Discuss the components of agile IT acquisition.
	8.2 LO 7: Using tools, methodologies and rules, evaluate the development acquisition model/plan for different acquisitions. Include the vehicle to be used (i.e., GSA schedule, unitary RFP or multiple awards).
Competency 8.3 - Post-award IT contract management	8.3 LO 1: List and describe post-award contract management methods and strategies that must be incorporated during the planning phase of the contract. Include methods of control, benchmarks, performance measurement, contract change management, termination strategies, and documentation of lessons learned.
	8.3 LO 2: Discuss the importance of pre-termination and termination decision points.
	8.3 LO 3: Discuss how to manage inter-agency partnering

	issues and relationships after a shared service contract has been awarded.
Competency 8.4 - IT acquisition best practices	8.4 LO 1: Discuss how to monitor and evaluate commercial and public sector IT acquisition best practices.
• OMB 25 Point Plan • OMB, OFPP memo on Guidance for Specialized IT Acquisition Cadres	8.4 LO 2: Discuss how to design, develop and use integrated program teams for IT acquisition.
.	8.4 LO 3: Discuss the utility of lease versus purchase analyses for IT acquisitions.
	8.4 LO 4: Discuss the utility of in-house versus out-sourced or shared IT services (e.g., "cloud," software as a service, and platform as a service).
	8.4 LO 5: Discuss the ramifications of Section 508 of the Rehabilitation Act on the acquisition of electronic and IT (E&IT) products and services. Include in the discussion web-based tools that help government purchasers determine and document Section 508 requirements that apply to a particular E&IT acquisition. (See also 9.2 LO 5.)
	8.4 LO 6: Discuss methods to ensure that the Contracting Officer's Representative (COR) or Contracting Officer's Technical Representative (COTR) receives the necessary support of the IT management team and identify best practices specific to the interface between the COTR and the contracting officer.
Competency 8.5 - Software acquisition management • OMB Circular A-11 • OMB Circular A-130 • SEI at Carnegie Mellon	8.5 LO 1: Discuss the elements to include in a well-defined agency policy for acquisition of software.
	8.5 LO 2: Discuss common causes of cost, schedule and performance problems associated with software procurement.
	8.5 LO 3: Apply requirements management and risk mitigation techniques associated with software acquisition.
	8.5 LO 4: Discuss software acquisition models and tools used to manage lifecycle planning.
	8.5 LO 5: Evaluate software performance measures and metrics. (See also 6.7 LO 5 and LO 6.)

	8.5 LO 6: Discuss the total cost of software acquisition, including license ownership and renewal.
Competency 8.6 - Supply chain risk management in acquisition	8.6 LO 1: Identify and define the different supply chain issues (including people, data, and suppliers) and their associated risks, including commodity IT.
	8.6 LO 2: Evaluate a supply chain model to ensure its service delivery is mission-focused, optimized, and mitigates risk.
	8.6 LO 3: Explore optional expansion of potential supply chains through federal exchanges and auctions.

9.0: Information and Knowledge Management	*General Discussion: Under Title 40, Subtitle III, Chapter 113, Section 11315, Agency CIOs have information resources management (IRM) identified as their primary responsibility. Per Circular A-130, IRM encompasses both information itself and the related resources, such as personnel, equipment, funds, and information technology. As part of their information management responsibilities, the CIO must also deal with Privacy issues; Freedom of Information Act (FOIA) requirements; Open Government mandates; and accessibility issues, as well as the preservation of records to comply with business, operating, regulatory and legal requirements. In addition, the CIO may support knowledge management activities to preserve and share subject matter expertise.*
Competency 9.1 - Privacy, personally identifiable, and protected health information	9.1 LO 1: Explain generally accepted definitions of privacy and security. Distinguish between privacy issues and security concerns.
• 5 U.S.C. 552 and 552a • Health Insurance Portability and Accountability Act (HIPAA) of 1996 • E-Government Act • OMB Circular A-130 • OMB M-99-18 • OMB M-01-05 • OMB M-03-22 • OMB M-06-15 • OMB M-06-16 • OMB M-06-19 • OMB M-07-16 • OMB M-10-23 • OMB M-11-02 • NIST SP 800-122	9.1 LO 2: Identify and discuss legislation, regulations and policies regarding privacy, personally identifiable information, and protected health information.
	9.1 LO 3: Evaluate security and privacy laws and regulations, including FOIA, relative to transparency and open government.
	9.1 LO 4: Assess internal and external factors affecting an organization's privacy policies and practices. Include discussion of challenges presented with social networking capabilities and social engineering techniques.
	9.1 LO 5: Discuss and give examples of the importance of planning, developing, and implementing, maintaining, and disposing of systems which address privacy. (See also 12.4 LO 3.)

• E-Government Act • OMB Circular A-11 • OMB Circular A-130	9.1 LO 6: Explain the Privacy Impact Assessment (PIA) process, the type of events which require a PIA, and the content of a PIA.
	9.1 LO 7: Identify and discuss privacy issues that may occur relative to other IT responsibilities such as records management, archival records, FOIA requests, declassification, firewalls, and security involving partners (extended enterprises).
	9.1 LO 8: Discuss the importance of encrypting data at rest and in transit with respect to personal privacy and social engineering attacks and exploits.
Competency 9.2 - Information accessibility • 29 U.S.C. 794d (Section 508 of the Rehabilitation Act of 1973, as amended) • U.S. Access Board Standards • Federal Acquisition Regulation (FAR), Part 10.000-10.002 • Federal Enterprise Architecture (FEA: Security and Privacy Profile • OMB memorandum of July 19, 2010, Improving the Accessibility of Government Information	9.2 LO 1: List and discuss the laws, standards and regulations relative to accessibility. (See also 4.2 LO 5, 6.7 LO 5.)
	9.2 LO 2: Describe electronic and information technology (E&IT) to which U.S. Code title 29, section 794d requirements apply and identify which E&IT are exempt from the law.
	9.2 LO 3: Describe the benefits, attributes and application of different types of adaptive technologies.
	9.2 LO 4: Discuss individual agency and designated federal roles and responsibilities (e.g., OMB, GSA, and Department of Justice) in implementing Section 508 requirements.
	9.2 LO 5: Discuss how the CIO can advocate for E&IT accessibility in all phases of web technology and software development planning, development and procurement. (See also 8.4 LO 5, 9.6 LO 11.)

Competency 9.3 - Records and information management	9.3 LO 1: Describe the full lifecycle of information management from creation or acquisition through its final disposition. This includes organizing, categorizing, classifying, disseminating, and migrating information.
• 44 U.S.C. Chapter 31 • 5 U.S.C. §552 and 552a • E-Government Act • OMB Circular A-130 • OMB M-12-18 • National Archives and Records Administration (NARA) regulations • ARMA International Standards and Best Practices for Excellence in Managing Records and Information • ISO 15489-1	9.3 LO 2: Discuss records management requirements established in statute and regulation.
• 5 U.S.C. §552 and 552a • OMB M-12-18	9.3 LO 3: Identify and discuss the impact of information and records management requirements on systems design.
	9.3 LO 4: Discuss the role of records management in developing and maintaining information resources that support business needs and processes.
	9.3 LO 5: Discuss how records and information management support the integrity, authenticity, preservation of electronic records. Include discussion of information assurance, privacy implications, and FOIA compliance.
	9.3 LO 6: Identify and analyze records management strategies that contribute to cost-effective, productive information services.
	9.3 LO 7: Identify records management issues associated with vital records and disaster recovery and how to address those issues in your agency.
	9.3 LO 8: Compare, contrast and evaluate knowledge management and records management tools.
	9.3 LO 9: Identify IT applications to accelerate electronic record keeping in agencies.
	9.3 LO 10: Discuss the e-discovery phase of civil/criminal litigation and CIOs' responsibilities for records retention and preservation.

Competency 9.4 - Knowledge management	*General Discussion: Knowledge Management (KM) involves the use of disciplined processes (and their supporting tools) to optimize application of knowledge in support of the organization's overall mission. KM involves linking people to people, people to content and content to content.*
	9.4 LO 1: Define Knowledge Management and discuss how it may be used to support the strategic goals of an organization.
	9.4 LO 2: Explain how KM can improve individual and organizational effectiveness.
	9.4 LO 3: Identify ways to develop a culture of knowledge sharing, collaboration and support of KM.
	9.4 LO 4: Identify and evaluate technological tools that may be used in implementing KM systems.
	9.4 LO 5: Evaluate approaches to measuring the effectiveness of KM efforts.
	9.4 LO 6: Compare the various roles that a CIO may assume in support of Knowledge Management.
	9.4 LO 7: Formulate a KM process that incorporates best practices.
Competency 9.5 - Social media	9.5 L0 1: Discuss the pros and cons of allowing the open use of social media in federal agencies.
	9.5 LO 2: Describe how social media is changing the way collaboration occurs in agencies.
	9.5 LO 3: Describe how crowdsourcing impacts "silos" in federal agencies.
	9.5 LO 4: Describe how the "personal you" and the "official you" should operate in the federal and private social media spaces.
	9.5 LO 5: Discuss the elements that should be included in an agency social media policy.
Competency 9.6 - Web development and maintenance strategy	9.6 LO 1: Explore the organizational implications and structure needed for web-based development.
• E-Government Act • Digital Millennium Copyright Act • OMB M-11-15	9.6 LO 2: Discuss approaches to web content management.
	9.6 LO 3: Compare and contrast agency web governance models.
	9.6 LO 4: Discuss the importance of maintaining a disciplined process for software configuration changes to web sites.

	(See also 6.1 LO 7.)
• OMB M-05-04 • OMB M-11-24 • OMB Memorandum of April, 7, 2010 on Social Media, Web-Based Interactive Technologies, and the Paperwork Reduction Act • Digital Government: Building a 21st Century Platform to Better Serve the American People	9.6 LO 5: Identify legislative and policy requirements for government web-based development.
• OMB M-10-23	9.6 LO 6: Evaluate build/buy partnership issues relative to web development.
• OMB M-10-22	9.6 LO 7: Discuss the use of web analytics in business decision making and customer/client satisfaction.
• OMB Memorandum of September 28, 2010 on Transition to IPV6	9.6 LO 8: Compare, contrast and evaluate a single agency approach to web services delivery versus a multi-agency portal with a common infrastructure.
	9.6 LO 9: Assess the impact of web development technologies on government shared services. (Also see Competency 12.4 on Web technology.)
	9.6 LO 10: Discuss the challenges of “apps” development and deployment within the Federal Government, including the use of application programming interfaces (API) to share information.
	9.6 LO 11: Analyze considerations related to privacy, security and accessibility in government web development. (See also 9.2 LO 1, 10.4 LO 4, and 12.4 LO 3.)

Competency 9.7 - Open government • President's Memorandum on Transparency and Open Government • President's Memorandum on Building a 21st Century Digital Government • Digital Government: Building a 21st Century Platform to Better Serve the American People • OMB M-10-06	9.7 LO 1: Discuss the drivers influencing digital government at the federal level.
	9.7 LO 2: Compare and contrast the nature of government-based public information transactions and those that occur in private industry.
• Digital Government: Building a 21st Century Platform to Better Serve the American People	9.7 LO 3: Discuss the role of federal CIOs in open government.
	9.7 LO 4: Discuss the pros and cons of how open government impacts accountability for public officials and government performance.
	9.7 LO 5: Discuss the impact of public engagement on regulation and regulatory review.
	9.7 LO 6: Assess best practices and metrics available to measure public participation in open government.
	9.7 LO 7: Discuss available technologies to improve efficiency and access to government information.
	9.7 LO 8: Discuss the challenges agencies may encounter in providing digital services.
	9.7 LO 9: Analyze potential security concerns associated with open government.
	9.7 LO 10: Examine the impact of platforms such as data.gov and provide examples of their benefits.

Competency 9.8 - Information collection • 44 U.S.C. Chapter 35 • OMB Circular A-130 • OMB M-10-22 • OMB Memorandum of April 7, 2010 on Information Collection under the Paperwork Reduction Act	9.8 LO 1: Discuss the statutory and regulatory requirements associated with information collection both internally within an organization and externally from the public.
	9.8 LO 2: Discuss potential information collection and privacy issues associated with surveying individuals. Include in the discussion the data collection, storage and ownership implications that may occur based on who is conducting the survey (i.e., the agency, inter-governmental organization, private firm, contractor or other commercial entity).

10.0: Cybersecurity/Information Assurance (IA) • Subchapter III of Chapter 35 of Title 44, U.S.C. • International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World • Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure • National Strategy to Secure Cyberspace • OMB Circular A-130 • NSTISSI 4011 • CNSSI 4012 • CNSSI 4014 • ISO 27000	*General Discussion: The Federal Information Security Management Act (FISMA) – codified in Chapter 35 of Title 44, U.S. Code - charges each Federal CIO with the responsibilities to develop and maintain an agency-wide cybersecurity/information assurance(IA) program, including security policies, procedures and control techniques to both protect and defend information, systems and networks. CIOs must be able to assess the risks associated with vulnerable systems and information; determine the levels of security protection required; institute cost-effective methods to reduce risk to acceptable levels; and continuously monitor the capabilities of those techniques and controls. In addition, they must oversee the training programs to ensure that both the protectors and users of information and systems have the knowledge necessary to adequately protect organizational assets. The Office of Management and Budget (OMB) promulgates procedures for FISMA compliance and has levied additional requirements for cybersecurity/IA programs through OMB Circular A-130. Additionally, there are legislative and regulatory requirements that mandate specific care for certain types of information including (but not limited to) sensitive but unclassified information, corporate fiduciary information, personally identifiable information, and personal health information.*
	10.0 LO 1: Explain the enterprise cybersecurity/IA risks, national security risks, challenges, and opportunities associated with the current and future cybersecurity/IA environment.
	10.0 LO 2: Describe the operational and financial impacts of breaches in security and loss of trust on the business/mission of an organization.

Competency 10.1 - CIO Cybersecurity/IA roles and responsibilities • Subchapter III of Chapter 35 of Title 44, U.S.C. • OMB M-10-28 • OMB M-11-29 • CNSSI 4012 • NIST SP 800-100 • CMU/SEI-2005-TN-023, Governing for Information Security • ISO/IEC 27002 • Open Group, Information Security Management Maturity Model (ISM3)	10.1 LO 1: Analyze the Federal Information Security Management Act, codified in Subchapter III of Chapter 35 of title 44, U.S. Code, and related implementing guidance, (including National Institute of Standards and Technology (NIST), Office Management and Budget (OMB), and Committee on National Security Systems (CNSS) criteria) to determine the cybersecurity/IA roles and responsibilities of senior managers responsible for information or information systems/technology.
• NIST SP 800-53A • NIST SP 800-100	10.1 LO 2: Identify recognized sources of cybersecurity/IA best practices to include computer emergency readiness teams (e.g., US-CERT, U.S. Cyber Command, SEI's CERT Coordination Center); standards, configurations, and methodologies bodies (e.g., NIST Special Publications, ISO standards, common criteria); public/private partnerships (e.g., Center for Internet Security(CIS)); federal auditing agencies, e.g., GAO; federal regulatory or coordination bodies, e.g., Federal Energy Regulatory Commission (FERC), National Infrastructure Coordination Center (NICC); and commercial security institutes.
	10.1 LO 3: Define the items that constitute basic cybersecurity/IA literacy necessary to be a senior manager responsible for information or information systems/technology.
	10.1 LO 4: Identify and evaluate resources needed to achieve an acceptable level of security and to remedy security risk deficiencies based on system criticality and information sensitivity.

Competency 10.2 - Cybersecurity/IA legislation, policies, and procedures • Chapter 35 of Title 44, U.S.C. • Section 209 of the E-Government Act • Chapter 9 of Title 31, U.S.C. • Health Insurance Portability and Accountability Act (HIPAA) of 1996 • NIST FIPS and Special Publications Series • CNSS Issuances • ICD 503 • NSD-42 • GAO-09-232G • OMB M-07-11 • OMB M-07-18 • National Initiative for Cybersecurity Education	10.2 LO 1: Explain the important implications from the array of legislation, regulations and standards related to cybersecurity and information assurance (IA).
• OMB M-06-16	10.2 LO 2: Discuss how to evaluate security management policies and practices to ensure that they are cost effective and effectively reduce risk.
	10.2 LO 3: Describe how to apply cybersecurity/IA concepts to ensure compliance with other applicable requirements, including those standards and guidelines for national security systems issued in accordance with law and as directed by the President.
• NIST SP 800-53	10.2 LO 4: Develop and describe how to implement a methodology to annually evaluate the effectiveness of cybersecurity/IA policies, procedures, and practices.
	10.2 LO 5: Demonstrate how cybersecurity/IA is addressed throughout the lifecycle of an agency's information system.
• • NIST SP 800-61 • ISO/IEC 27002 • ISO/PAS 22399 • ITIL, Incident Management Open Guide • CMU/SEI-2007-TR-008	10.2 LO 6: Evaluate procedures for detecting, reporting, and responding to security incidents, to ensure that they are consistent with standards and guidelines issued pursuant to 44 U.S.C. 3546(b).
Competency 10.3 - Cybersecurity/IA Strategies and Plans	10.3 LO 1: Using a business case, evaluate the IA strategy for a major or critical IT system.
	10.3 LO 2: Evaluate the potential return on investment from technical countermeasures employed to meet security

	requirements.
	10.3 LO 3: Within an enterprise architectural framework, identify interdependency relationships and the associated impact resulting from cybersecurity/IA breach or compromise.
	10.3 LO 4: Discuss the need for procedural cybersecurity/IA safeguards during an IT acquisition process.
Competency 10.4 - Information and information systems threats and vulnerabilities analysis • CNSSI 4014	10.4 LO 1: Explain the use of the operations security (OPSEC) cycle (identifying critical information, analyzing threats, analyzing vulnerabilities, assessing risk, and applying countermeasures) for implementing a security system that protects information about a mission, operations or activity (thus denying or mitigating an adversary's ability to compromise or interrupt that mission, operation or activity).
• 6 U.S.C. 485 • CNSSI 4014	10.4 LO 2: Examine the inherent security challenges associated with implementing cross-agency information sharing capabilities. (See also 1.5 LO 2.)
• CNSSI 4014	10.4 LO 3: Analyze the security implications of software and hardware assurance, as it applies to confidentiality, and integrity, including legislation dealing with source manufacturing. Include internal GOTS, external COTS, internet/intranet, legacy codes, applicable legislation regarding source manufacturing, and the types of individuals (U.S. trained, foreign national H-1B visa holders, off-shore workforce, etc.) developing software.
	10.4 LO 4: Explain security issues and interdependencies related to various technologies and their impact on the security architecture of an organization. (See also 9.6 LO 11.)
• NSPD-54/HSPD-23 • OMB M-11-06 • NIST SP 800-42 • NSA Security Configuration Guides • DISA STIGs • http://sectools.org	10.4 LO 5: Formulate strategies to defend against the actions of state-sponsored attackers, hackers, hactivists, organized crime, industrial and international cyber espionage, advanced persistent threats, supply chain, and insider cyber threats.
	10.4 LO 6: Explain the role of human factors in cybersecurity/IA. Include human computer interaction, design, training, sabotage, human error prevention and error identification, personal use policies and monitoring, and internal contractor integrity.
• NIST SP 800-137	10.4 LO 7: Discuss how to develop and implement continuous monitoring practices.
• OMB M-06-16	10.4 LO 8: Explain the challenges and requirements

	associated with both logical and physical security of mobile and remotely-accessed information.
• NIST SP 800-37	10.4 LO 9: Evaluate security considerations and risks associated with emerging technology.
• NIST SP 800-37 • NIST SP 800-53	10.4 LO 10: Discuss how to address cybersecurity/IA requirements during technology transitions.
	10.4 LO 11: List and discuss available computer incident response assistance. Include US-CERT, Department of Energy's Computer Incident Response Capability, the U.S. Secret Service's National Threat Assessment Center, U.S. Cyber Command, the CERT Coordination Center and commercial services available to the Federal Government.
• OMB M-07-16	10.4 LO 12: Discuss breach notification requirements and how to effectively implement supportive agency procedures.
• OMB Federal Cloud Computing Strategy • NIST SP 500-291 • NIST SP 800-146 • GAO-10-513 • NSA, Cloud Computing – Overview of Information Assurance Concerns and Opportunities • Cloud Security Alliance for Critical Areas in Cloud Computing • GSA, Cloud IT Services	10.4 LO 13: Understand and evaluate the operational and financial benefits/tradeoffs of emerging technologies, and associated cybersecurity/IA benefits/tradeoffs, with respect to the use of virtualization capabilities, and cloud capabilities that deliver software, platform, or infrastructure as a service. (See also 12.7 LO 5.)
• OMB Federal Cloud Computing Strategy	10.4 LO 14: Discuss the security considerations of, and best practices for, "cloud" services (e.g., NIST, Cloud Security Alliance, ENISA, and Open Group's Jericho Forum). (See also 12.7 LO 5.)
• Federal Risk and Authorization Management Program (FedRAMP)	10.4 LO 15: Discuss the assessment and authorization (A&A) process related to cloud computing services and products. (See also 12.7 LO 5.)
	10.4 LO 16: Discuss the security requirements and risks associated with using service oriented architectures.

Competency 10.5 - Information security controls planning and management • Chapter 35 of Title 44, U.S.C. • 40 U.S.C. 11331 • NIST SP 800-53 (and associated publications) • FIPS PUB 199 • FIPS PUB 200 • CNSSI 4012 • CNSSI 4014 • OMB Circular A-130	10.5 LO 1: Determine the levels of cybersecurity/IA appropriate to protect an organization's information, information systems, and networks in accordance with standards promulgated under 40 U.S.C. 11331.
	10.5 LO 2: Explain the concepts of confidentiality, integrity, and availability as applied to Information Systems Security.
• CNSSI 4014	10.5 LO 3: Explain the use and types of security controls as directed in federal policies and procedures.
• CNSSI 4012	10.5 LO 4: Based on a risk analysis, select the security controls or other means to mitigate risks from unauthorized access, use, denial of service, disruption, modification, or destruction of information and information systems.
	10.5 LO 5: Develop a security plan and evaluate its compliance with agency and federal regulations for protection of the confidentiality, integrity, and availability of information, information systems, and networks. Discuss how to continually update the plan to incorporate lessons learned from prior incidents, address emerging technologies, and reflect evolving best practices.
• National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy • HSPD-12 • OMB M-11-11	10.5 LO 6: Explain the standards for employer and contractor identification prior to gaining physical access to federally controlled facilities and logical access to federally controlled information systems.
	10.5 LO 7: Describe how to evaluate the performance of security controls and techniques to ensure that they are effectively implemented (includes testing those security controls and techniques). Discuss current federal-wide initiatives.

Competency 10.6 - Cybersecurity/IA risk management • Chapter 35 of Title 44, U.S.C. • OMB Circular A-130, Appendix III • NIST SP 800-30 • NIST SP 800-37 • NIST SP 800-39 • NIST SP 800-53 • NIST SP 800-59 • CNSSI 4012 • ISO/IEC 27005	10.6 LO 1: Assess the risk and magnitude of the operational and financial harm that could result from the unauthorized access, use, disclosure, disruption, modification, denial of service, or destruction of agency information and information systems.

• NIST SP 800-37 • NIST SP 800-53	10.6 LO 2: Specify responsibilities and criteria for granting approvals.
• NIST SP 800-37 • NIST SP 800-53	10.6 LO 3: Develop implementing procedures for granting authority to operate (i.e., certification and accreditation).
• NIST SP 800-37 • NIST SP 800-53	10.6 LO 4: Formulate risk management plans to mitigate identified cybersecurity/IA weaknesses.
Competency 10.7 - Enterprise-wide cybersecurity/IA program management • Chapter 35 of Title 44, U.S.C. • OMB Circular A-130, Appendix III • NIST SP 800-100	10.7 LO 1: Evaluate an agency-wide cybersecurity/IA program and modify the program to comply with changes in policies, laws, regulations, standards, threats, and vulnerabilities.
	10.7 LO 2: Model how to document remedial action to address deficiencies in the cybersecurity/IA policies, procedures, and practices of an organization.
• Chapter 35 of Title 44, U.S.C. • NIST SP 800-16 • NIST SP 800-50 • CNSSI 4012 • ISO/IEC 27002	10.7 LO 3: Develop a plan and implementing procedures for a comprehensive cybersecurity/IA education and training program that includes tiered levels of training (e.g., general managers, personnel with significant responsibilities for information security, and general agency awareness training), as well as continuous learning requirements.
Competency 10.8 - Information security reporting compliance • Chapter 35 of Title 44, U.S.C. • OMB M-12-20 (or latest FY guidance) • OMB Guidance on Exhibit 300	10.8 LO 1: Discuss OMB IT security reporting requirements and develop an example of such a report.
• OMB M-11-33 • OMB M-12-20 • NIST SP 800-137	10.8 LO 2: Discuss the Department of Homeland Security's agency requirements for continuous monitoring and reporting through Cyberscope. (See also 10.4 LO 7.)
	10.8 LO 3: Develop policies to identify and comply with intrusion reporting requirements.
	10.8 LO 4: Develop the security and privacy sections for a business case.

Competency 10.9 - Critical infrastructure protection and disaster recovery planning • Chapter 35 of Title 44, U.S.C. • HSPD-7 • HSPD-8 • NSPD-51/HSPD-20 • National Strategy for the Physical Protection of Critical Infrastructures and Key Assets • National Infrastructure Protection Plan (NIPP • DHS, National Response Framework • OMB Circular A-130, Appendix III	10.9 LO 1: Explain concerns regarding the protection and safeguarding of America's critical infrastructures, both governmental and commercial, including power, transportation, banking and telecommunications systems. Include in the discussion key homeland security laws and policies, global trade practices and other efforts to protect and maintain America's physical and cyber infrastructures.
	10.9 LO 2: Discuss the disaster recovery planning process and its place within the overall continuity of operations and business continuity management process. (See also Competency 4.4 on Contingency and continuity of operations planning (COOP.))
	10.9 LO 3: Discuss the major elements involved in disaster recovery planning ranging from dealing with the emergency situation to recovery.

11.0: Enterprise Architecture • Federal Enterprise Architecture (FEA) • FEA Framework (FEAF) • FEA Reference Model • GAO-10-846G	*General Discussion: An enterprise architecture (EA) establishes the agency-wide roadmap(s) to meet mission and strategic goals through the optimal performance of core business processes and supporting information resources (e.g. systems, applications, databases, websites, and networks). Enterprise architecture roadmaps are essential for transforming the existing business processes and IT solutions to an optimal business capability target that provides maximum mission value. EA includes agile plans for transitioning from the current business and technology operating environment to the target environment.*
	11.0 LO 1: Explain the multi-dimensional nature of how enterprise architecture describes and documents the existing and target enterprise, how architecture supports the organization's current and future mission, and why architectures must be agile in order to support changing conditions.
	11.0 LO 2: Describe business reasons for developing an enterprise architecture (EA) and discuss benefits that can be derived from successful implementation of a sound EA.
Competency 11.1 - Enterprise architecture functions and governance	11.1 LO 1: Identify and describe roles in an EA program, such as those for the Executive Sponsor, Chief Information Officer, Chief (or Enterprise) Architect, Solutions Architects, Data Architects, and Systems Architects.
	11.1 LO 2: Describe the symbiotic relationship between strategic planning and EA and their impacts on visionary planning, portfolio management, and IT governance.
• Subtitle III of Title 40, U.S.C. • Chapters 35 and 36 of Title 44, U.S.C. • E-Government Act • OMB Circular A-130 • OMB Circular A-11 • Federal Enterprise Architecture (FEA) • FEA Framework (FEAF) • FEA Reference Model • GAO-10-846G	11.1 LO 3: Describe and discuss impacts of key regulatory requirements and guidance as they relate to enterprise architecture.
	11.1 LO 4: Describe the role of the Federal Enterprise Architecture (FEA) and how it contributes to cross-agency architecture practices.

	11.1 LO 5: Discuss the role of the Federal CIO Council in influencing agency EA practices.
	11.1 LO 6: Identify the EA responsibilities of internal agency managerial boards and committees and how they contribute to the agency's business and technology governance processes.
	11.1 LO 7 Describe how EA governance and EA planning provide complementary roles and discuss the benefits of integrated governance and planning processes.
Competency 11.2 - Key enterprise architecture concepts	11.2 LO 1: Identify and describe the purpose of the main elements of an enterprise architecture, including drivers, analysis, strategic direction, baseline and agile targets, focused road maps, alignment to services, programs and portfolios, work products, standards and best practices.
	11.2 LO 2: Describe the major EA components and how they are used in decision making, prioritization and budgetary processes.
	11.2 LO 3: Describe the relationship between EA and emerging technologies and standards, as well as the use of accepted standards.
	11.2 LO 4: Compare and contrast the dimensions and benefits of different architectural frameworks.
• FEA • FEAF	11.2 LO 5: Describe the purpose and use of reference models in enterprise architecture development and how they bring value to the decision making, prioritization, and budgetary processes.
	11.2 LO 6: Describe how the FEA reference models and profiles can be used to support agency IT program analysis and annual status reporting.
	11.2 LO 7: Identify EA best practices for each level of the architecture and demonstrate how to apply them in practical ways to optimize IT portfolios, programs and services.
	11.2 LO 8: Discuss the need to integrate security and privacy requirements into the EA. Include issues such as cross-realm security, security consequences of aggregated architectural data, common identity management approaches, data loss prevention and revocation/repudiation mechanisms.

Competency 11.3 - Enterprise architecture interpretation, development, and maintenance • OMB, Improving Agency Performance Using Information and Information Technology (Enterprise Architecture Assessment Framework)	11.3 LO 1: Discuss how to assess an agency's baseline architecture in terms of its effectiveness in meeting enterprise/strategic goals and performance goals and identify gaps that should be addressed.
	11.3 LO 2: Describe basic architecture documentation (i.e., work product) methodologies at each level of a commonly used framework (e.g., Federal Enterprise Architecture Framework (FEAF), the Department of Defense Architecture Framework (DODAF), or the Zachman Framework).
	11.3 LO 3: Discuss the purpose and value of automated tools to document, analyze, and monitor the enterprise architecture.
	11.3 LO 4: Discuss the importance and key aspects of model interpretation in understanding and sharing metadata, integration and component reuse, and achieving interoperability.
	11.3 LO 5: Discuss the benefits and importance of understanding the history of an organization's architecture and the business cases that were used to support it.
	11.3 LO 6: Discuss the relationship between the strategic planning process and EA and how linking these disciplines improves IT portfolios and operations. (See also 5.1 LO 6.)
	11.3 LO 7: Compare, contrast and evaluate internal and external drivers for new and emerging technology and their business implications.

Competency 11.4 - Use of enterprise architecture in IT investment decision making	11.4 LO 1: Discuss the importance of mapping major IT capital investments to the organization's strategic goals and business line activities, as well as alignment with an agency's target architecture.
	11.4 LO 2: Discuss how to achieve buy-in from Line of Business owners and senior executives to maintain sufficient resources for an effective EA program.
	11.4 LO 3: Describe how to resolve competing architectural principles to ensure best practices are maintained and architectural analysis remains useful in the decision making process.
	11.4 LO 4: Describe how an integrated capital planning and EA process can improve mission performance in spite of continually changing IT and agency requirements.
• FEA • OMB Circular A-11 • OMB Circular A-130	11.4 LO 5: Describe the relationship between the practical implementation of Federal Enterprise Architecture Reference Models and an agency's capital planning and investment control process. Include a discussion of related sections of OMB Circulars A-11 and A-130.
Competency 11.5 - Enterprise data management	11.5 LO 1: Describe the basic components of a data management program.
	11.5 LO 2: Discuss the criticality of data interoperability and quality to enterprise-wide information exchange, and the role of data standardization in supporting interoperability.
	11.5 LO 3: Describe current federal information exchange standards that are used and their role in intra- and inter-governmental sharing of information.
	11.5 LO 4: Discuss how the data architecture can be used to prioritize the elements of a data management program.
	11.5 LO 5: Describe the attributes of data quality and how architectural practices can improve data quality and application development within an agency.
• FEA Consolidated Reference Model	11.5 LO 6: Compare and contrast the differences between data management and records management and how they may support one another.
Competency 11.6 - Performance measurement for enterprise architecture	11.6 LO 1: Define and describe performance goals and distinguish performance goals from performance standards.
• FEA Consolidated Reference Model	11.6 LO 2: Discuss and describe the role of IT performance goals and standards with respect to the enterprise/program strategic plan, general goals and performance goals.

	11.6 LO 3: Discuss how automated network, security, and application monitoring tools can be used for trend analysis and establishing performance indicators as part of a CIO's "dashboard." (See also 5.3 LO 2, 5.5 LO 3, and 5.6 LO 1.)

12.0: Technology Management and Assessment • OPM ECQ 4	*General Discussion: Since the inception of the Clinger-Cohen Act, the CIO's role as technology manager has become increasingly complex. The ability to ensure effective development and deployment of technology requires a broad awareness of current and emerging technology capabilities, standards, policies and law. CIOs must also be able to identify and evaluate the strategic benefits of technology applications within the business environment.*
Competency 12.1 - Network, telecommunications, and mobile device technology	12.1 LO 1: Explain data transmission concepts, functions, and mechanisms.
	12.1 LO 2: Explain the capabilities and limitations of data transmission modes and media.
	12.1 LO 3: Evaluate the benefits and limitations of commonly-used local wired and wireless voice and data communication architectures, devices, and protocols.
• NIST SP 800-153	12.1 LO 4: Evaluate the benefits and limitations of commonly-used wide-area wired and wireless voice and data architectures, networks, devices and protocols.
• Digital Government: Building a 21st Century Platform to Better Serve the American People	12.1 LO 5: Describe how broader laws, policies and standards have been impacted by evolving mobile technology.
	12.1 LO 6: Discuss the processes and tools associated with developing, testing and distributing mobile applications.
	12.1 LO 7: Discuss the key elements required for effective mobile device management within an organization.
• Digital Government: Building a 21st Century Platform to Better Serve the American People • A Toolkit to Support Federal Agencies Implementing Bring Your Own Device Program	12.1 LO 8: Debate the pros and cons of implementing a "bring your own device" (BYOD) program.
Competency 12.2 - Spectrum management	12.2 LO 1: Define spectrum and evaluate the relationship between federal agency missions and spectrum management.
• FCC National Broadband Plan	12.2 LO 2: Assess the potential impacts on spectrum availability and management arising from increased domestic and international demand.
• FCC National Broadband Plan • NTIA Manual of Regulations and	12.2 LO 3: Identify and discuss federal and international laws and regulations that govern spectrum management.

Procedures for the Federal Radio Frequency Management	
	12.2 LO 4: Identify and evaluate tools and techniques available for effective spectrum management.
	12.2 LO 5: Identify recognized sources of best practices in spectrum-efficient technologies.
	12.2 LO 6: List and discuss spectrum management architecture issues and interdependencies.
	12.2 LO 7: Discuss supportability requirements that must be met prior to acquisition or modification of a new/existing telecommunications system.
Competency 12.3 - Computer systems	12.3 LO 1: Develop a plan for managing competing priorities among the portfolio of future hardware initiatives.
	12.3 LO 2: Investigate methods for managing hardware obsolescence.
	12.3 LO 3: Articulate a process for judging when to upgrade hardware based on emerging software requirements.
	12.3 LO 4: Demonstrate how to manage transitions from legacy systems.
	12.3 LO 5: Describe strategies to manage the changing integration among software.
Competency 12.4 - Web technology	12.4 LO 1: Review World Wide Web Consortium standards and discuss how they impact web technology development.
	12.4 LO 2: Define Extensible Markup Language (XML) standards and use. Relate the XML standards to the Federal Enterprise Architecture (FEA) Data Reference Model (DRM).
• OMB M-10-22	12.4 LO 3: Discuss the impact of web technology on privacy. (See also 9.1 LO 5 and 9.6 LO 11.)
	12.4 LO 4: Define and evaluate the use of Service Oriented Architectures (SOA) as they relate to web technology development. Relate SOA to the Federal Enterprise Architecture (FEA) Service Component Reference Model (SRM).
	12.4 LO 5: Define and evaluate industry best practices related to development and maintenance of SOA services.
	12.4 LO 6: Explain how performance metrics are used to measure the effectiveness of web technology development and deployment.
	12.4 LO 7: Discuss the challenges and opportunities associated with integrating new technologies and

	applications into the Federal Government's IT infrastructure.
Competency 12.5 - Data management technology	12.5 LO 1: Discuss the evolution of database management systems and the implications of various structural approaches.
	12.5 LO 2: Discuss the complexities associated with big data.
	12.5 LO 3: Describe best practices associated with data warehouse management.
	12.5 LO 4: Outline the rationale behind data mining and describe the varied uses of data mining.
	12.5 LO 5: Describe the benefits and challenges of enterprise business intelligence.
	12.5 LO 6: Detail the roles of XML and Radio Frequency Identification (RFID) in data management.
	12.5 LO 7: Discuss Online Analytical Processing (OLAP) and the associated benefit of the use of multidimensional information.
Competency 12.6 - Software development technology	12.6 LO1: Discuss how SOA enables the development and use of new web services that can support integration and governance requirements.
	12.6 LO 2: Compare the benefits and limitations of open source software with vendor developed software.
	12.6 LO 3: Outline the criteria for determining whether to use COTS or other types of software. (See also Competency 6.7 on Software development, testing and implementation.)
	12.6 LO 4: Discuss the evolution of enterprise resource planning (ERP) and customer relationship management (CRM), as well as major ERP and CRM implementation challenges.
	12.6 LO 5: Describe the objectives of software assurance, and how best to incorporate them into an information technology organization.
	12.6 LO 6: Discuss software as a service, and outline the criteria for deciding to purchase software in this manner.
	12.6 LO 7: Discuss the range of applications made possible by geographic information systems.

Competency 12.7 - Cloud Computing • NIST SP 800-145 • NIST SP 800-146	12.7 LO 1: Define cloud computing, the general cloud environments, and service models.
• NIST SP 800-146	12.7 LO 2: Outline the criteria for deciding to use cloud computing services.
	12.7 LO 3: Discuss the challenges associated with implementing identity and access standards across the cloud.
• NIST SP 800-144	12.7 LO 4: Discuss privacy implications and develop principles for a privacy framework within the cloud.
• NIST SP 800-53 • NIST SP 800-144	12.7 LO 5: Evaluate information security considerations and risks associated with cloud computing. (See also 10.4 LO 13, 14, and 15.)
	12.7 LO 6: Discuss data management and reliability issues associated with cloud computing.
	12.7 LO 7: Discuss the challenges associated with cloud deployment and migration.
	12.7 LO 8: Discuss cloud reliability and continuity of operations.
• OMB Federal Cloud Computing Strategy	12.7 LO 9: Discuss public and private sector cloud computing initiatives.
Competency 12.8 - Special use technology	12.8 LO 1: Define, discuss and investigate the use of Supervisory Control and Data Acquisition Systems (SCADA) in government systems.
	12.8 LO 2: Define metrics to assess the effectiveness of SCADA systems used in contractor systems.
	12.8 LO 3: Discuss the use of collaborative technology within the Federal Government.
	12.8 LO 4: Define metrics to assess the effective use of collaborative technology at all government levels.
	12.8 LO 5: Investigate industry best practices using collaborative technology to support global management and data exchange.
	12.8 LO 6: Define, discuss and investigate the use of modeling and simulation technology.
	12.8 LO 7: Describe how gamification can be used to address various challenges faced by the Federal Government.

	12.8 LO 8: Define, discuss and evaluate Human Computer Interface (HCI) technology.
	12.8 LO 9: Define metrics to assess the effective use of HCI technology in government systems.
	12.8 LO 10: Discuss and evaluate the capabilities of biometric-based personal identification/verification technology.
	12.8 LO 11: Discuss and evaluate the capabilities of the most common forms of social media.
Competency 12.9 - Emerging technology	12.9 LO1: Evaluate internal and external information sources of information on new and emerging technologies and their business implications.
	12.9 LO 2: Discuss approaches to aligning agency regulations and policies with emerging technologies and behavioral trends.
	12.9 LO 3: Describe strategies for managing competing priorities among the portfolio of future hardware (and related software) initiatives.
	12.9 LO 4: Describe how disruptive technologies support innovation and their impact, both positive and negative, on the business marketplace.

Appendix A - List of References

American National Standards Institute (ANSI)	**American National Standards Institute/Project Management Institute (ANSI/PMI) 99-001-2008:** Guide to the Project Management Body of Knowledge (PMBOK Guide) **American National Standards Institute/Electronic Industries Alliance (ANSI/EIA)-748:** Earned Value Management Systems
Committee on National Security Systems Instruction (CNSSI)	**CNSSI 4012:** National Information Assurance Training Standard for Senior System Managers **CNSSI 4014**: National Information Assurance Training Standard for Information Systems Security Officers
Department of Homeland Security	National Infrastructure Protection Plan, 2009 National Response Framework, January 2008 National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, February 2003
Federal Chief Information Officers Council	Federal CIO Council Charter A Toolkit to Support Federal Agencies Implementing Bring Your Own Device Programs, August 23, 2012
Federal Communications Commission (FCC)	National Broadband Plan
Federal Continuity Directive (FCD)	**FCD 1:** Federal Executive Branch National Continuity **FCD 2:** Federal Executive Branch Mission Essential Functions and Primary Mission Essential Functions
Federal Information Processing Standards (FIPS) Publication (PUB)	**FIPS PUB 199:** Standards for Security Categorization of Federal information and Information Systems **FIPS PUB 200:** Minimum Security Requirements for Federal Information and Information Systems
Government Accountability Office (GAO)	**GAO Investment Guide** **GAO-04-394G:** Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity **GAO-09-3SP:** GAO Cost Estimating and Assessment Guide **GAO-09-232G:** Federal Information Systems Controls Audit Manual (FISCAM) **GAO-10-513:** Federal Guidance Needed to Address Control Issues with Implementing Cloud Computing **GAO-10-846G:** Organizational Transformation: A Framework for Assessing and Improving Enterprise Architecture Management
Homeland Security Presidential Directive (HSPD)	**HSPD-7:** Critical Infrastructure Identication, Prioritization and Protection **HSPD-8:** National Preparedness **HSPD-12:** Policy for a Common Identification Standard for Federal Employees and Contractors **NSPD-51/HSPD-20:** National Continuity Policy **NSPD-54/HSPD-23:** Comprehensive National Cybersecurity Initiative
International Organization for Standardization (ISO)	**ISO 9000 series:** Quality Management **ISO 9001:** Quality Management Systems

	ISO/IEC 9126: Software Engineering – Product Quality **ISO/IEC 12207:** Systems and Software Engineering – Software Lifecycle Processes **ISO 15489-1:** Information and Documentation: Records Management **ISO/PAS 22399:** Guideline for Incident Preparedness and Operational Continuity Management **ISO/IEC 27000:** Information Security Management Systems Family of Standards **ISO/IEC 27002:** Information Security: Code of Practice for Information Security Management **ISO/IEC 27005:** Information Technology -- Security Techniques -- Information Security Risk Management **ISO 31000:** Risk Management Family of Standards **ISO 38500:** Corporate Governance of Information Technology
Intelligence Community Directive (ICD)	**ICD 503:** Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation
National Communications System Directive (NCSD)	**NCSD 3-10:** Minimum Requirements for Continuity Communications Capabilities
National Institute of Standards and Technology (NIST) Special Publication (SP)	**NIST SP 500-291:** NIST Cloud Computing Standards Roadmap **NIST SP 800-30:** Risk Management Guide for Information Technology Systems **NIST SP 800-34:** Contingency Planning Guide for Federal Information Systems **NIST SP 800-37:** Information Security: Guide for Applying the Risk Management Framework to Federal Information Systems **NIST SP 800-39:** Managing Information Security Risk - Organization, Mission, and Information System View **NIST SP 800-42:** Guideline on Network Security Testing **NIST SP 800-53:** Recommended Security Controls for Federal Information Systems and Organizations **NIST SP 800-53A**: Information Security: Guide for Assessing the Security Controls in Federal Information Systems **NIST SP 800-59:** Guideline for Identifying an Information System as a National Security System **NIST SP 800-61:** Computer Security Incident Handling Guide **NIST SP 800-65:** Information Security: Integrating IT Security into the Capital Planning and Investment Control Process **NIST SP 800-100:** Information Security Handbook: A Guide for Managers **NIST SP 800-122:** Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) **NIST SP 800-125:** Guide to Security for Full Virtualization Technologies **NIST SP 800-128:** Guide for Security-Focused Configuration Management of Information Systems **NIST SP 800-137:** Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations **NIST SP 800-144:** Guidelines on Security and Privacy in Public Cloud Computing **NIST SP 800-145:** The NIST Definition of Cloud Computing **NIST SP 800-146:** Cloud Computing Synopsis and Recommendations **NIST SP 800-153:** Guidelines for Securing Wireless Local Area Networks
National Security Directive (NSD)	**NSD 42:** National Policy for the Security of National Security Telecommunications and Information Systems
Office of Management and Budget (OMB) Circulars	**Circular A-11:** Preparation, Submission, and Executive of the Federal Budget **Circular A-94:** Guidelines and Discount Rates for Benefit-Cost Analysis of Federal

	Programs **Circular A-123:** Management's Responsibility for Internal Control **Circular A-127:** Financial Management Systems **Circular A-130:** Management of Federal Information Resources **Circular A-135:** Management of Federal Advisory Committees
OMB Guidance	Enterprise Architecture Assessment Framework (EAAF) Federal Enterprise Architecture (FEA) Consolidated Reference Model FEA Practice Guidance, November 2007 OMB Guidance on Exhibit 53: Information Technology and E-Government OMB Guidance on Exhibit 300: Planning, Budgeting, Acquisition and Management of Information Technology Capital Assets
OMB Numbered Memoranda	**M-99-18:** Privacy Policies on Federal Web Sites **M-01-05:** Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy **M-03-22:** OMB Guidance for Implementing the Privacy Provisions of th E-Government Act of 2002 **M-05-04:** Policies for Federal Agency Public Websites **M-05-08:** Designation of Senior Agency Officials for Privacy **M-06-15:** Safeguarding Personally Identifiable Information (PII) **M-06-16:** Protection of Sensitive Agency Information **M-06-19:** Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments **M-07-11:** Implementation of Commonly Accepted Security Configurations for Windows Operating Systems **M-07-16:** Safeguarding Against and Responding to the Breach of Personally Identifiable Information **M-07-18:** Ensuring New Acquisitions Include Common Security Configurations **M-09-02:** Information Technology Management Structure and Governance Framework **M-09-12:** President's Memorandum on Transparency and Open Government – Interagency Collaboration **M-10-06:** Open Government Directive **M-10-22:** Guidance for Online Use of Web Measurement and Customization Technologies **M-10-23:** Guidance for Agency Use of Third-Party Websites and Applications **M-10-27:** Information Technology Investment Baseline Management Policy **M-10-28:** Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS) **M-11-02:** Sharing Data While Protecting Privacy **M-11-06:** WikiLeaks – Mishandling of Classified Material **M-11-11:** Continued Implementation of HSPD-12 – Policy for a Common Identification Standard for Federal Employees and Contractors **M-11-15:** Final Guidance on Implementing the Plain Writing Act of 2010 **M-11-17:** Delivering on the Accountable Government Initiative and Implementing the GPRA Modernization Act of 2010 **M-11-24:** Implementing Executive Order 13571 on Streamlining Service Delivery and Improving Customer Service **M-11-26:** New Fast Track Process for Collecting Service Delivery Feedback Under the Paperwork Reduction Act

	M-11-29: Chief Information Officer Authorities **M-12-06:** 2012 Discount Rates for OMB Circular No. A-94 **M-12-09:** President's Memorandum on Transparency and Open Government – Interagency Collaboration **M-12-10:** Implementing PortfolioStat **M-12-18:** Managing Government Records Directive **M-12-20:** FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management
OMB Unnumbered Memoranda	**April 7, 2010:** Social Media, Web-Based Interactive Technologies, and the Paperwork Reduction Act **April 7, 2010:** Information Collection under the Paperwork Reduction Act **July 19, 2010:** Improving the Accessibility of Government Information **September 28, 2010:** Transition to IPV6 **July 13, 2011:** Guidance for Specialized Information Technology Acquisition Cadres
OMB Reports/Strategies	**June 2009**: Improving Agency Performance Using Information and Information Technology (Enterprise Architecture Assessment Framework) **December 9, 2010:** 25 Point Implementation Plan to Reform Federal Information Technology Management **February 8, 2011:** Federal Cloud Computing Strategy
Office of Personnel Management (OPM) Executive Core Qualifications (ECQ)	**ECQ 1 – Leading Change:** This ECQ involves the ability to bring about strategic change, both within and outside the organization, to meet organizational goals. Inherent to this ECQ is the ability to establish an organizational vision and to implement it in a continuously changing environment. Included in this ECQ are the competencies of creativity and innovation, external awareness, flexibility, resilience, strategic thinking, and vision. **ECQ 2 – Leading People:** This ECQ involves the ability to lead people toward meeting the organization's vision, mission, and goals. Inherent to this ECQ is the ability to provide an inclusive workplace that fosters the development of others, facilitates cooperation and teamwork, and supports constructive resolution of conflicts. Included in this ECQ are the competencies of conflict management, leveraging diversity, developing others, and team building . **ECQ 3 – Results Driven:** This ECQ involves the ability to meet organizational goals and customer expectations. Inherent to this ECQ is the ability to make decisions that produce high-quality results by applying technical knowledge, analyzing problems, and calculating risks. Included in this ECQ are the competencies of accountability, customer service, decisiveness, entrepreneurship, problem solving, and technical credibility. **ECQ 4 – Business Acumen:** This ECQ involves the ability to manage human, financial, and information resources strategically. Included in this ECQ are the competencies of financial management, human capital management, and technology management. **ECQ 5 – Building Coalitions:** This ECQ involves the ability to build coalitions internally and with other Federal agencies, State and local governments, nonprofit and private sector organizations, foreign governments, or international organizations to achieve common goals. Included in this ECQ are the competencies of partnering, political savvy, and influencing/negotiating.

Presidential Executive Orders (EO)	**EO 13231:** Critical Infrastructure Protection in the Information Age **EO 13388:** Further Strengthening the Sharing of Terrorism Information to Protect Americans **EO 13526:** Classified National Security Information **EO 13556:** Controlled Unclassified Information **EO 13576:** Delivering an Efficient, Effective, and Accountable Government **EO 13589:** Promoting Efficient Spending
Presidential Memoranda	**January 21, 2009:** President Barack Obama, Memorandum on Transparency and Open Government **May 23, 2012:** President Barack Obama, Memorandum Building a 21st Century Digital Government
Presidential Policy Directives (PPD)	**PPD-1:** Organization of the National Security Council System
White House Strategies	Digital Government: Building a 21st Century Platform to Better Serve the American People, May 23, 2012 National Strategy for Information Sharing: Success and Challenges in Improving Terrorism-Related Information Sharing, 2009 National Strategy for Trusted Identities in Cyberspace, April 2011
United States Code	**5 U.S.C. §552:** The Freedom of Information Act, as amended by Public Law No. 104-231, 110 Stat. 3048 **5 U.S.C. §552a:** Records Maintained on Individuals **6 U.S.C. §485:** Information Sharing **29 U.S.C. §794d**: Section 508 of the Rehabilitation Act of 1973, as amended **31 U.S.C. Chapter 9:** Chief Financial Officers Act of 1990 **40 U.S.C. Subtitle III:** Information Technology Management (includes codified Clinger-Cohen Act) **44 U.S.C. Chapter 31:** Records Management by Federal Agencies **44 U.S.C. Chapter 35:** Coordination of Federal Information Policy (includes codified Paperwork Reduction Act) **44 U.S.C. Chapter 36:** Management and Promotion of Electronic Government Services
Other Statutes	E-Government Act of 2002 Federal Advisory Committee Act Federal Acquisition Streamlining Act of 1994, (PL 103-355), Title V, Acquisition Management Government Performance and Results (GPRA) Modernization Act of 2010 Statutory Pay-As-You-Go Act of 2010 (Title I of Public Law 111-139)
Miscellaneous	ARMA International Standards and Best Practices for Excellence in Managing Information and Records Department of Defense Acquisition Risk Management Guide, 6th Edition, Version 1.0 Defense Information Systems Agency Security Technical Implementation Guide (DISA STIG)

National Security Agency (NSA) Security Configuration Guides

National Telecommunications and Information Administration (NTIA) Manual of Regulations and Procedures for the Federal Radio Frequency Management

Regulations of National Archives and Records Administration (NARA) (see Subchapter B of 36 Code of Federal Regulations Chapter XII)

U.S. Intelligence Community, Information Sharing Policy

DHS Sensitive Systems Policy Directive 4300A

Version 8.0

March 14, 2011

This is the implementation of
DHS Management Directive 140-01 Information
Technology System Security, July 31, 2007

DEPARTMENT OF HOMELAND SECURITY

This page intentionally left blank

FOREWORD

The Department of Homeland Security (DHS) 4300 series of information security policy is the official series of publications relating to Departmental standards and guidelines adopted and promulgated under the provisions of DHS Management Directive 140-01 Information Technology System Security.

Comments concerning DHS Information Security publications are welcomed and should be submitted to the DHS Director for Information Systems Security Policy at INFOSEC@dhs.gov or addressed to:

DHS Director of Information Security Policy
OCIO CISO Stop 0182
Department of Homeland Security
245 Murray Lane SW
Washington, DC 20528-0182

Robert C. West
DHS Chief Information Security Officer

TABLE OF CONTENTS

1.0 INTRODUCTION

This document articulates the Department of Homeland Security (DHS) Information Security Program policies for sensitive systems. Procedures for implementing these policies are outlined in a companion publication, DHS 4300A *Sensitive Systems Handbook*. The handbook serves as a foundation for Components to develop and implement their information security programs. The baseline security requirements (BLSRs) included in the handbook must be addressed when developing and maintaining information security documents.

1.1 Information Security Program

The DHS Information Security Program provides a baseline of policies, standards, and guidelines for DHS Components. This document provides direction to managers and senior executives for managing and protecting sensitive systems. It also outlines policies relating to management, operational, and technical controls necessary for ensuring confidentiality, integrity, availability, authenticity, and nonrepudiation within the DHS information system infrastructure and operations. Policy elements are designed to be broad in scope. Specific implementation information can often be found in specific National Institute for Standards and Technology (NIST) publications, such as NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Systems and Organizations*.

The policies and direction contained in this document apply to all DHS Components. Information security policies and implementing procedures for National Security Systems are covered in separate publications, *DHS National Security Systems Policy Directive 4300B and DHS 4300B National Security Systems Handbook*. These publications are available on the DHS Chief Information Security Officer (CISO) website.

Policy elements are effective when issued. Any policy elements that have not been implemented within ninety (90) days shall be considered a weakness and either a system or program Plan of Action and Milestones (POA&M) must be generated by the Component for the identified weaknesses. Whenever the DHS Security Compliance tools, Risk Management System (RMS) and TrustedAgent FISMA (TAF) require updating to reflect policy element changes, tool changes shall be available to the Department within forty-five (45) days of the policy changes.

1.2 Authorities

The following list provides the authoritative references for the DHS sensitive information security program. Additional references are located in Appendix C of this document.

- Public Law 107-347, E-Government Act of 2002, including Title III, Federal Information Security Management Act (FISMA)
- Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*
- DHS Management Directive (MD) 140-01, *Information Technology Security Services*
- NIST Federal Information Processing Standards (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*
- NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*

1.3 Policy Overview

DHS information security policies delineate the security management structure and foundation to measure progress and compliance. Policies in this document are organized under three areas:

- **Management Controls** – Focus on managing both the system information security controls and system risk. These controls consist of risk mitigation techniques and concerns normally addressed by management.
- **Operational Controls** – Focus on mechanisms primarily implemented and executed by people. These controls are designed to improve the security of a particular system, or group of systems and often rely on management and technical controls.
- **Technical Controls** – Focus on security controls executed by information systems. These controls provide automated protection from unauthorized access or misuse. They facilitate detection of security violations, and support security requirements for applications and data.

1.4 Definitions

The following definitions apply to the policies and procedures outlined in this document. Other definitions may be found in the National Information Assurance (IA) Glossary, as well as the Privacy Incident Handling Guidance and the Privacy Compliance documentation.

1.4.1 Classified National Security Information

Information that has been determined, pursuant to Executive Order 13526, *Classified National Security Information*, to require protection against unauthorized disclosure and is marked to indicate its classified status.

1.4.2 National Intelligence Information

The following definition is provided in *Public Law 108-458, Intelligence Reform and Terrorism Prevention Act of 2004*, December 17, 2004, "The terms 'national intelligence' and 'intelligence related to national security' refer to all intelligence, regardless of the source from which derived and including information gathered within or outside the United States, that – "(A) pertains, as determined consistent with any guidance issued by the President, to more than one United States Government agency; and "(B) that involves – (i) threats to the United States, its people, property, or interests; (ii) the development, proliferation, or use of weapons of mass destruction; or (iii) any other matter bearing on United States national or homeland security."

1.4.3 National Security Information

Information that has been determined, pursuant to Executive Order 13526, *Classified National Security Information*, or any predecessor order, to require protection against unauthorized disclosure.

1.4.4 Foreign Intelligence Information

This type of information relates to the capabilities, intentions, and activities of foreign powers, organizations, or persons, but does not include counterintelligence except for information on international terrorist activities.

1.4.5 Sensitive Information

Sensitive information is information not otherwise categorized by statute or regulation that if disclosed could have an adverse impact on the welfare or privacy of individuals or on the welfare or conduct of Federal programs or other programs or operations essential to the national interest. Examples of sensitive information include personal data such as Social Security number; trade secrets; system vulnerability information; pre-solicitation procurement documents, such as statements of work; and law enforcement investigative methods; similarly, detailed reports related to computer security deficiencies in internal controls are also sensitive information because of the potential damage that could be caused by the misuse of this information. System vulnerability information about a financial system shall be considered Sensitive Financial Information. All sensitive information must be protected from loss, misuse, modification, and unauthorized access.

With the exception of certain types of information protected by statute (e.g., Sensitive Security Information, Critical Infrastructure Information), there are no specific Federal criteria and no standard terminology for designating types of sensitive information. Such designations are left to the discretion of each individual Federal agency. "For Official Use Only" (FOUO) is the term used within DHS to identify unclassified information of a sensitive nature that is not otherwise categorized by statute or regulation. DHS will adopt the term "Controlled Unclassified Information" (CUI) at a later date.

1.4.6 Public Information

This type of information can be disclosed to the public without restriction but requires protection against erroneous manipulation or alteration (e.g., Public Web sites).

1.4.7 Information Technology

The Clinger-Cohen Act defines information technology (IT) as any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an Executive agency.

For purposes of the preceding definition, "equipment" refers to that used by any DHS Component or contractor, if the contractor requires the use of such equipment in the performance of a service or the furnishing of a product in support of DHS.

The term "information technology" includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.

The term "information system," as used within this policy document, is equivalent to the term "IT system."

1.4.8 DHS System

A DHS system is any information system that transmits, stores, or processes data or information and is (1) owned, leased, or operated by any DHS Component, (2) operated by a contractor on behalf of DHS, or (3) operated by another Federal, state, or local Government agency on behalf of DHS. DHS systems include general support systems and major applications.

1.4.8.1 General Support System

A general support system (GSS) is an interconnected set of information resources under the same direct management control that share common functionality. A GSS normally includes hardware,

software, information, applications, communications, data and users. Examples of a GSS include a local area network (LAN), including smart terminals that support a branch office, a Department-wide backbone, a communications network, or a Departmental data processing center including its operating system and utilities.

Note: Security for GSS in use at DHS Headquarters shall be under the oversight of the DHS Office of the Chief Information Officer (OCIO), with support from the DHS Enterprise Operations Center (EOC). All other GSS shall be under the direct oversight of the respective Component CISOs, with support from the appropriate Component Security Operations Center (SOC). All GSS must have an Information Systems Security Officers (ISSO) assigned.

1.4.8.2 Major Application

A major application (MA) is an automated information system (AIS) that "requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.[1]" Note: All Federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. An MA is distinguishable from a GSS by the fact that it is a discrete application, whereas a GSS may support multiple applications. Each MA must be under the direct oversight of a Component CISO/Information System Security Manager (ISSM), and must have anISSO assigned.

1.4.9 Component

A DHS Component is any of the entities within DHS, including all DHS offices and independent agencies.

1.4.10 Trust Zone

A Trust Zone consists of a group of people, information resources, data systems, and/or networks subject to a shared security policy (set of rules governing access to data and services). For example, a Trust Zone may be set up between different network segments that require specific usage policies based on information processed, such as law enforcement information.

1.4.11 Continuity of Operations

Internal organizational efforts to ensure that a viable capability exists to continue essential functions across a wide range of potential emergencies, through plans and procedures that:

- Delineate essential functions and supporting information systems
- Specify succession to office and the emergency delegation of authority
- Provide for the safekeeping of vital records and databases
- Identify alternate operating facilities
- Provide for interoperable communications
- Validate the capability through tests, training, and exercises

[1] OMB Circular A-130

1.4.12 Continuity of Operations Plan

A plan that provides for the continuity of essential functions of an organization in the event that an emergency prevents occupancy of its primary facility. It provides the organization with an operational framework for continuing its essential functions when normal operations are disrupted or otherwise cannot be conducted from its primary facility.

1.4.13 Essential Functions

Functions that enable Federal Executive Branch agencies to provide vital services, exercise civil authority, maintain the safety and well being of the general populace, and sustain the industrial/economic base during an emergency.

1.4.14 Vital Records

Electronic and hardcopy documents, references, records, databases, and information systems needed to support essential functions under the full spectrum of emergencies. Categories of these types of records may include:

- *Emergency operating records* – emergency plans and directive(s), orders of succession, delegations of authority, staffing assignments, selected program records needed to continue the most critical agency operations, as well as related policy or procedural records.
- *Legal and financial rights* records – protect the legal and financial rights of the Government and of the individuals directly affected by its activities. Examples include accounts receivable records, social security records, payroll records, retirement records, and insurance records. These records were formerly defined as "rights-and-interests" records.
- *Records used to perform national security preparedness functions and activities (Executive Order [E.O.] 12656).*

1.4.15 Operational Data

Operational data is information used in the execution of any DHS mission.

1.4.16 Federal Information Security Management Act

FISMA requires each agency to develop, document, and implement an agency-wide information security program to provide a high-level of security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. Statutory requirements include:

(1) Periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency.

(2) Policies and procedures that:

a. Are based on the risk assessments required by paragraph (1) above

b. Cost-effectively reduce information security risks to an acceptable level

c. Ensure that information security is addressed throughout the life cycle of each agency information system

d. Ensure compliance with

i. Other Federal policies and procedures as may be prescribed by OMB and NIST, or other agencies when appropriate

ii. Minimally acceptable system configuration requirements, as determined by the agency

iii. Any other applicable requirements, including standards and guidelines for national security systems issued in accordance with law and as directed by the President

(3) Subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate;

(4) Security awareness to inform personnel, including contractors, others working on behalf of DHS, and other users of information systems that support operations and assets of the Department, of:

a. Information security risks associated with their activities

b. Their responsibilities in complying with agency policies and procedures designed to reduce these risks

(5) Periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually. This testing:

a. Shall include testing of management, operational, and technical controls of every information system identified in the Department's inventory

b. May include testing relied on by the Office of Inspector General;

(6) A process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices of the Department

(7) Procedures for detecting, reporting, and responding to security incidents, consistent with standards and guidelines promulgated by the United States Computer Emergency Readiness Team (US-CERT)

a. Mitigating risks associated with incidents before substantial damage is done

b. Notifying and consulting with the US-CERT

c. Notifying and consulting with:

i. Law enforcement agencies and relevant Offices of Inspector General

ii. An office designated by the President for any incident involving a national security system

iii. Other agency or offices, as required

(8) Plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the Department

FISMA requires the Chief Information Officer (CIO) to designate a senior agency information security official who shall develop and maintain a Department-wide information security program as required by the statute. Responsibilities include:

- Developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements
- Training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities
- Assisting senior Department officials concerning their responsibilities under the statute
- Ensuring that the Department has trained personnel sufficient to assist the Department in complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines; and
- Ensuring that the Department CIO, in coordination with other senior Department officials, reports annually to the Department head on the effectiveness of the Department information security program, including progress of remedial actions

1.4.17 Personally Identifiable Information

Personally Identifiable Information (PII) is any information that permits the identity of an individual to be directly or indirectly inferred, including any information which is linked or linkable to that individual regardless of whether the individual is a U.S. Citizen, lawful permanent resident, a visitor to the U.S., or employee or contractor to the Department.

1.4.18 Sensitive Personally Identifiable Information

Sensitive PII is PII which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Examples of Sensitive PII include Social Security numbers, alien number (A-number), criminal history information, and medical information. Sensitive PII requires stricter handling guidelines due to the sensitivity of the information.

1.4.19 Privacy Sensitive System

A Privacy Sensitive System is any system that collects, uses, disseminates, or maintains PII or Sensitive PII.

1.4.20 Strong Authentication

Strong authentication is a layered authentication approach relying on two or more authenticators to establish the identity of an originator or receiver of information.

1.4.21 Two-Factor Authentication

Authentication can involve something the user knows (e.g., a password), something the user has (e.g., a smart card), or something the user “is” (e.g., a fingerprint or voice pattern). Single-factor authentication uses only one of the three forms of authentication, while two-factor authentication uses any two of the three forms. Three-factor authentication uses all three forms.

1.5 Waivers and Exceptions

1.5.1 Waivers

Components may request waivers to, or exceptions from, any portion of this policy, for up to six (6) months, any time they are unable to fully comply with policy requirements. Requests are made, through the Component's ISSO for the system, to the Component's CISO/ISSM, and then to the DHS CISO. All submitters shall coordinate with the AO prior to submission. If a material weakness is reported in an audit report, and the control weakness is not scheduled to be remediated within twelve (12) months, the Component must submit a waiver request to the DHS CISO. If the material weakness is against a financial system, the Component Chief Financial Officer (CFO) must also approve the waiver request before sending to the DHS *CISO*.

In all cases waivers shall be requested for an appropriate period based on a reasonable remediation strategy.

1.5.2 Exceptions

Components may request an exception whenever they are unable to bring a system control weakness into compliance or when it requires a permanent exception to DHS policy. Exceptions are generally limited to systems that are unable to comply due to detrimental impact to mission, excessive costs, and/or clearly documented end of platform life for non-essential systems within eighteen (18) months, commercial-off-the-shelf (COTS) products that cannot be configured to support the control requirement. This request is made, through the Component CISO/ISSM, to the DHS CISO. All submitters shall coordinate with the AO prior to submission.

The resulting risk also must be approved and accepted by the Authorizing Official (AO) and by the Component CFO if the system is a financial or mixed financial system.

1.5.3 Waiver or Exception Requests

The Waivers and Exceptions Request Form, located in Attachment B of the DHS 4300A *Sensitive Systems Handbook*, shall be used.

Component ISSOs, audit liaisons, and others may develop the waiver or exception request, but the System Owner shall submit the request through the Component's CISO/ISSM.

Waiver requests shall include the operational justification (document mission impact), risk acceptance, risk mitigation measures, and a POA&M for bringing the system procedures or control weakness into compliance.

Exception requests shall include the operational justification (document mission impact), as well as efforts to mitigate the risk based to include descriptions of counter measures or compensating controls currently in place.

Any waiver or exception requests for CFO Designated Systems must be submitted to and approved by the Component's CFO prior to the DHS CFO's submission to the DHS CISO. Any waiver or exception requests for Privacy Sensitive Systems must be submitted to and approved by the Component's Privacy Officer or Senior Privacy Point of Contact (PPOC) prior to being submitted to the DHS CISO.

All approved waiver and exception requests must be directed through the Component's CISO/ISSM who will in turn direct it to the DHS CISO.

Policy ID	DHS Policy Statements	Relevant Controls
1.5.3.a	Systems without an Authorization to Operate (ATO) when this policy is issued shall comply with all of its policy statements or obtain appropriate waivers and/or exceptions.	PL-1
1.5.3.b	Systems with an ATO when this policy is issued shall comply with all of its policy statements within ninety (90) days or obtain appropriate waivers and/or exceptions. (A new ATO is only required for significant changes.)	PL-1
1.5.3.c	Each waiver or exception request shall include the system name, and system TrustedAgent FISMA (TAF) Inventory ID, operational justification, and risk mitigation.	CM-3
1.5.3.d	Components shall request a waiver whenever they are *temporarily* unable to comply fully with any portion of this policy.	CA-2
1.5.3.e	All waiver requests shall identify the POA&M for bringing the system or program into compliance.	CA-5, PM-4
1.5.3.f	The Component CISO/ISSM shall approve all waiver requests prior to submitting them to the DHS CISO.	CA-6
1.5.3.g	Requests submitted without sufficient information shall be returned for clarification prior to making a decision.	CA-6
1.5.3.h	A waiver shall be issued for six (6) months or less. The DHS CISO reserves the right to issue waivers for longer than six (6) months in exceptional situations. Waivers may be renewed by following the same process as in the initial request.	CA-2
1.5.3.i	The Head of the Component shall approve any waiver request that results in a total waiver time exceeding twelve (12) months before sending it to the DHS CISO. The waiver shall also be reported as a material weakness in the Component's FISMA report.	---
1.5.3.j	Components shall request an exception whenever they are permanently unable to comply fully with any portion of this policy.	CA-2
1.5.3.k	All approved waivers shall be reported in the Component's FISMA report.	CA-6
1.5.3.l	The DHS CFO shall approve all requests for waivers and exceptions for financial systems prior to their submission to the DHS CISO.	CA-6
1.5.3.m	The Component's Privacy Officer or Senior PPOC shall approve all requests for waivers and exceptions for Privacy Sensitive Systems prior to their submission to the DHS CISO.	

1.5.4 U.S. Citizen Exception Requests

Special procedures apply for exception to the requirement that persons accessing DHS systems be U.S. Citizens. Under normal circumstances, only U.S. Citizens are allowed access to DHS systems and networks; however at times there is a need to grant access to foreign nationals. Access for foreign nationals is normally a long-term commitment, and exceptions to appropriate policies are treated separately from standard exceptions and waivers. The approval chain for an exception to the U.S. Citizenship requirement flows through the Component Head, the Office of Security, and the CIO. An electronic form for requesting exceptions to the U.S. Citizenship requirement is published in Attachment J of the *DHS 4300A Sensitive Systems Handbook*.

Policy ID	DHS Policy Statements	Relevant Controls
1.5.4.a	Persons of dual citizenship, where one of the citizenships includes U.S. Citizenship, shall be treated as U.S. Citizens for the purposes of this directive.	---
1.5.4.b	The System Owner shall submit each request for exception to the U.S. Citizenship policy to the Component Head. The Component Head shall obtain concurrence from the DHS Chief Security Officer (CSO) and CIO prior to the approval becoming effective.	PS-3
1.5.4.c	Additional compensating controls shall be maintained for foreign nationals, based on nations lists maintained by the DHS CSO.	PS-3

1.6 Information Sharing and Electronic Signature

The DHS Enterprise Operations Center (EOC) exchanges information with Component SOCs, Network Operations Centers (NOCs), the Homeland Secure Data Network (HSDN) SOC, the Intelligence Community, and with external organizations in order to facilitate the security and operation of the DHS network. This exchange enhances situational awareness and provides a common operating picture to network managers. The operating picture is developed from information obtained from "raw" fault, configuration management, accounting, performance, and security data. This data is monitored, collected, analyzed, processed, and reported by the NOCs and SOCs.

The DHS EOC is responsible for communicating other information such as incident reports, notifications, vulnerability alerts and operational statuses to the Component SOCs, Component CISOs/ISSMs or other identified Component points of contact.

The DHS EOC portal implements role-based user profiles that allow Components to use the website's incident database capabilities. Users assigned to Component groups shall be able to perform actions such as:

- Entering incident information into the DHS EOC incident database
- Generating preformatted incident reports
- Initiating queries of the incident database
- Viewing FISMA incident reporting numbers

- Automating portions of the Information Security Vulnerability Management (ISVM) program
- Automating portions of the vulnerability assessment program

Policy ID	DHS Policy Statements	Relevant Controls
1.6.a	For DHS purposes, electronic signatures are preferred to pen and ink or facsimile signatures in all cases, except where pen and ink signatures are required by public law, Executive Order, or other agency requirements.	---
1.6.b	Components are encouraged to use electronic signatures whenever possible.	---
1.6.c	Components shall accept electronic signatures whenever the signature's digital certificate is current, electronically verifiable, and issued by a medium or high assurance DHS Certification Authority (CA) or other medium or high CA under the Federal Bridge Certification Authority (FBCA) or Common Authority.	---
1.6.d	DHS and Component systems shall be able to verify PIV credentials issued by other Federal agencies.	

1.7 Changes to Policy

Procedures and guidance for implementing this policy are outlined in a companion publication, *DHS 4300A Sensitive Systems Handbook* with attachments. The handbook serves as a foundation for Components to use in developing and implementing their information security programs.

For interpretation or clarification of DHS information security policies found in this policy document and of the procedures and guidance found in the *DHS 4300A Sensitive Systems Handbook*, contact the DHS CISO at infosec@dhs.gov.

Changes to this policy and to the handbook may be requested by submitting the form included in *DHS 4300A Sensitive Systems Handbook Attachment P – Document Change Requests* to the respective ISSM/CISO.

Policy ID	DHS Policy Statements	Relevant Controls
1.7.a	The DHS CISO shall be the authority for interpretation, clarification, and modification of the *DHS Sensitive Systems Policy Directive 4300A* and the *DHS 4300A Sensitive Systems Handbook* (inclusive of all appendices and attachments).	PL-1
1.7.b	The DHS CISO shall update the *DHS Sensitive Systems Policy Directive 4300A* and the *DHS 4300A Sensitive Systems Handbook* at least annually.	PL-1

2.0 ROLES AND RESPONSIBILITIES

Security is an inherently Governmental responsibility; contractors, others working on behalf of DHS, and other sources may assist in the performance of security functions, but a DHS employee must always be designated as the responsible agent for all security requirements and functions. This section outlines the roles and responsibilities for implementing these requirements.

2.1 Information Security Program Roles

Designated personnel play a major role in the planning and implementation of information security requirements. Roles directly responsible for information system security are described in the following subsections.

2.1.1 DHS Senior Agency Information Security Officer

Policy ID	DHS Policy Statements	Relevant Controls
2.1.1.a	The DHS CISO shall perform the duties and responsibilities of the DHS Senior Agency Information Security Officer (SAISO).	PL-1, PM-2

2.1.2 DHS Chief Information Security Officer

The DHS CISO shall implement and manage the DHS Information Security Program to ensure compliance with applicable Federal laws, Executive Orders, directives, policies, and regulations.

The DHS CISO reports directly to the DHS CIO and is the principal advisor for information security matters.

Policy ID	DHS Policy Statements	Relevant Controls
2.1.2.a	The DHS CISO shall implement and manage the DHS-wide Information Security Program.	PL-1, PM-2
2.1.2.b	The DHS CISO will serve as the CIO's primary liaison with the organization's authorizing officials, information system owners and ISSOs.	---

The DHS CISO:

Implements and manages the Department-wide Information Security Program and ensures compliance with FISMA, OMB, and other Federal requirements

- Issues Department-wide information security policy, guidance, and architecture requirements for all DHS systems and networks. These policies shall incorporate NIST guidance, as well as all applicable OMB memoranda and circulars
- Facilitates development of subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems

- Serves as the principal Departmental liaison with organizations outside the DHS for matters relating to information security
- Reviews and approves the tools, techniques, and methodologies planned for use in certifying and accrediting DHS systems, and for reporting and managing systems-level FISMA data. This includes Security Assessment plans, Contingency Plans, and security risk assessments.
- Consults with the DHS CSO on matters pertaining to physical security, personnel security, information security, investigations, and Sensitive Compartmented Information (SCI) systems, as they relate to information security and infrastructure
- Develops and implements procedures for detecting, reporting, and responding to information security incidents
- Ensures preparation and maintenance of plans and procedures to provide continuity of operations for information systems
- Ensures that Department personnel, contractors, and others working on behalf of DHS receive appropriate information security awareness
- Chairs the CISO Council. This Council is comprised of all Component CISOs, and is the Department's sole coordination body for any issues associated with information security policy, management, and operations. Component ISSMs will be invited to CISO Council meetings as required
- Maintains a comprehensive inventory of all GSS and MA in use within the Department
    - Security management for every GSS shall be under the direct oversight of either the DHS CISO (for enterprise systems) or a Component CISO/ISSM (for Component-specific general support systems)
    - MAs must be under the direct control of either a Component CISO or Component ISSM
- Maintains a repository for all Information Assurance (IA) Security Authorization process documentation and modifications
- Performs security reviews for all planned information systems acquisitions over $2.5 million and additional selected cases
- Provides oversight of all security operations functions within the Department
- Maintains classified threat assessment capability in support of security operations
- Performs annual program assessments for each of the Components
- Performs periodic compliance reviews for selected systems and applications
- Publishes monthly compliance scorecards
- Delegates specific authorities and responsibilities for maintaining a high degree of compliance to Component CISOs and ISSMs, as appropriate
- Reports annually to the Secretary on the effectiveness of the Department information security program, including progress of remedial actions. This report provides the primary basis for the Secretary's annual FISMA report to both OMB and to the United States Congress.

- Assists senior Department officials concerning their responsibilities under FISMA
- Heads an office with the mission and resources to assist in ensuring Department compliance with information security requirements
- Appoints a DHS employee to serve as the Headquarters CISO
- Appoints a DHS employee to serve as the Office of Intelligence and Analysis (I&A) CISO
- Provide operational direction to the DHS SOC

2.1.3 Component Chief Information Security Officer

The Component CISO implements and manages all aspects of the Component Information Security Program to ensure compliance with DHS policy and guidance that implement FISMA, other laws, and Executive Orders.

Policy ID	DHS Policy Statements	Relevant Controls
2.1.3.a	Component CISOs shall develop and maintain a Component-wide information security program in accordance with the DHS security program.	PL-1, PM-2
2.1.3.b	All Components shall be accountable to the appropriate CISO. Components without a fulltime CISO shall be responsible to the HQ CISO.	---

The following Components shall have a fulltime CISO:

- Customs and Border Protection
- Immigration and Customs Enforcement
- Transportation Security Administration
- United States Secret Service
- United States Coast Guard
- Federal Emergency Management Agency
- United States Citizenship and Immigration Services
- Federal Law Enforcement Training Center
- Headquarters, Department of Homeland Security
- Intelligence and Analysis

Component CISOs:

- Oversee the Component information security program
- Ensure that the Component CIO is kept apprised of all pertinent matters involving the security of information systems

- Ensure that information security-related decisions and information, including updates to the 4300 series of information security publications, are distributed to the ISSOs and other appropriate persons within their Component
- Approve and/or validate all Component information system security reporting
- Consult with the Component Privacy Officer or PPOC for reporting and handling of privacy incidents
- Manage information security resources including oversight and review of security requirements in funding documents
- Review and approve the security of hardware and software prior to implementation into the Component SOC
- Provide operational direction to the Component SOC
- Periodically test the security of implemented systems
- Implement and manage a POA&M process for remediation by creating a POA&M for each known vulnerability
- Ensure that ISSOs are appointed for each information system managed at the Component level. Review and approve ISSO appointments
- Ensure that weekly incident reports are submitted to the DHS EOC
- Acknowledge receipt of ISVM messages, report compliance with requirements or notify the granting of waivers
- Manage Component firewall rule sets
- Ensure that Interconnection Security Agreements (ISAs) are maintained for all connections between systems that do not have the same security policy
- Ensure execution of the DHS Logging Strategy detailed in the *DHS 4300A Sensitive Systems Handbook*
- Ensure adherence to the DHS Secure Baseline Configuration Guides (DHS 4300A Sensitive Systems Handbook, Enclosure 1)
- Ensure reporting of vulnerability scanning activities to the DHS EOC as detailed in *Attachment O, Vulnerability Management Program*, of *DHS 4300A Sensitive Systems Handbook*
- Develop and maintain a Component-wide information security program in accordance with Department policies and guidance
- Implement Department information security policies, procedures, and control techniques to address all applicable requirements
- Ensure training and oversight for personnel with significant responsibilities for information security
- Oversee the Security Authorization process for GSSs and MAs in use within the Component
    - Maintain an independent Component-wide Assessment program to ensure a consistent approach to testing of effectiveness of controls

- Ensure that an appropriate SOC performs an independent network assessment as part of the assessment process for each application that is accredited
- Ensure that enterprise security tools are utilized

- Exercise oversight over all Component security operations functions, including the Component SOCs

  Ensure that eternal providers who operate information systems on behalf of the Component meet the same security requirements as the Component with an acceptable level of trust in the external service, or else use compensating controls to constrain the nature of information or the process flow, accept a greater degree of risk, or decline the service and reduce functionality

Component CISO qualifications include:

- Possess professional qualifications, including training and experience, required to administer the functions described, including maintaining a Top Secret/Sensitive Compartmented Information (TS/SCI) clearance
- Have information security duties as that official's primary duty
- Participate in the DHS CISO Council, chaired by the DHS CISO
- Head an office with the mission and resources to assist in ensuring Component compliance with this directive and to coordinate, develop, implement, and maintain an organization-wide information security program
- Serve as the Component Risk Executive

2.1.4 Component Information Systems Security Manager

Components that are not required to have a fulltime CISO shall have a fulltime Information Systems Security Manager (ISSM). The ISSM is designated in writing by the Component CIO, with the concurrence of the HQ CISO.

Policy ID	DHS Policy Statements	Relevant Controls
2.1.4.a	Component ISSMs shall serve as the principal interface between the HQ CISO, Component ISSOs and other security practitioners.	---
2.1.4.b	The Component ISSM shall work directly with the HQ CISO.	---

The ISSM plays a critical role in ensuring that the DHS Information Security Program is implemented and maintained throughout the Component.

Component ISSMs:

- Oversee the Component information security program
- Ensure that the Component CIO and HQ CISO are kept apprised of all pertinent matters involving the security of information systems

- Ensure that information security-related decisions and information, including updates to the 4300 series of information security publications, are distributed to the ISSOs and other appropriate persons within their Component
- Validate all Component information system security reporting
- Consult with the Component Privacy Officer or PPOC for reporting and handling of privacy incidents
- Manage information security resources including oversight and review of security requirements in funding documents
- Periodically test the security of implemented systems
- Implement and manage a POA&M process for remediation by creating a POA&M for each known vulnerability
- Ensure that ISSOs are appointed for each information system managed at the Component level
- Ensure that weekly incident reports are forwarded to the HQ CISO
- Acknowledge receipt of Information Security Vulnerability Management (ISVM) messages, report compliance with requirements or notify the granting of waivers
- Ensure adherence to the DHS Secure Baseline Configuration Guides (DHS 4300A Sensitive Systems Handbook, Enclosure 1)
- Develop and publish procedures necessary to implement the requirements of DHS information security policy within the appropriate Component
- Implement Department information security policies, procedures, and control techniques to address all applicable requirements
- Ensure training and oversight for personnel with significant responsibilities for information security
- Oversee the Security Authorization process for MAs in use within the Component
    - Maintain an independent Component-wide ST&E Program to ensure a consistent approach to testing of effectiveness of controls
    - Ensure that an appropriate SOC performs an independent network assessment as part of the ST&E process for each application that is accredited
    - Ensure that enterprise security tools are utilized

2.1.5 Risk Executive

A Risk Executive ensures that risks are managed consistently across the organization. In keeping with its organizational structure, DHS has two levels of Risk Executives – Departmental and Component. The risk executive provides a holistic view of risk beyond that associated with the operation and use of individual information systems. Risk Executive inputs are documented and become part of the security authorization decision. All DHS Risk Executives:

- Ensure that managing information system-related security risks is consistent across the organization, reflects organizational risk tolerance, and is performed as part of an organization-wide process that considers other organizational risks affecting mission/business success
- Ensure that information security considerations for individual information systems, including the specific authorization decisions for those systems, are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization
- Provide visibility into the decisions of authorizing officials and a holistic view of risk to the organization beyond the risk associated with the operation and use of individual information systems
- Facilitate the sharing of security-related and risk-related information among authorizing officials and other senior leaders within the organization in order to help these officials consider all types of risks that may affect mission and business success and the overall interests of the organization at large

The DHS Risk Executive develops information security policy, establishes the standards for system security risk, oversees risk management and monitoring, and approves all waivers and exceptions to DHS policy.

The Component Risk Executives may establish standards for system security risk more stringent than the DHS standard. They implement the system security risk management and monitoring program and submit requests for higher-risk deviations from the enterprise standard.

Policy ID	DHS Policy Statements	Relevant Controls
2.1.5.a	The DHS CIO shall be the DHS Risk Executive. (The DHS CISO has been designated by the DHS CIO as the Risk Executive.)	PL-1, PM-9
2.1.5.b	Each Component CISO shall be the Risk Executive within his or her Component.	PL-1, PM-9
2.1.5.c	The Risk Executive shall perform their duty in accordance with NIST SP 800-37.	

2.1.6 Authorizing Official

The Authorizing Official (AO) formally assumes responsibility for operating an information system at an acceptable level of risk. He or she shall be a senior management official and a Federal employee or military member. The Authorizing Official will also assign the Security Control Assessor for the system.

Policy ID	DHS Policy Statements	Relevant Controls
2.1.6.a	The DHS CIO shall act as the AO for enterprise information systems or shall designate one in writing.	CA-6

Policy ID	DHS Policy Statements	Relevant Controls
2.1.6.b	The Component CIO shall act as the AO for Component information systems or shall designate one in writing.	CA-6
2.1.6.c	Every system shall have a designated AO. (An AO may be responsible for more than one system.)	CA-6
2.1.6.d	The AO shall review and approve any individual requiring administrator privileges. The AO may delegate this duty to the appropriate system owner or Program Manager.	AC-2
2.1.6.e	The AO shall be responsible for acceptance of resulting risk to organizational operations and assets, individuals, other organizations, and the Nation.	CA-6
2.1.6.f	The AO shall periodically review security status to determine if risk remains acceptable	CA-6
2.1.6.g	The AO shall perform additional duties in accordance with NIST SP 800-37	CA-6

2.1.7 Security Control Assessor

The Security Control Assessor is a senior management official who certifies the results of the security assessment. A Certifying Official is assigned in writing to each information system by an appropriate Component official, typically the Component Head or Component CIO. He or she shall be a Federal employee.

The Security Control Assessor and the team conducting a certification must be impartial, that is, free from any perceived or actual conflicts of interest with respect to the developmental, operational, and/or management chain of command associated with the information system or to the determination of security control effectiveness.

For systems with low impact, a Security Control Assessor and/or certifying team do not need to be independent so long as assessment results are carefully reviewed and analyzed by an independent team of experts to validate their completeness, consistency, and veracity.

The AO decides the required level of certifier independence based on the criticality and sensitivity of the information system and the ultimate risk to organizational operations, organizational assets, and individuals. The AO determines if the level of certifier independence is sufficient to provide confidence that the assessment results produced are sound and can be used to make credible, risk-based decisions.

Policy ID	DHS Policy Statements	Relevant Controls
2.1.7.a	The Component CISO shall serve as Security Control Assessor when no other person has been officially designated.	CA-2
2.1.7.b	A Security Control Assessor may be responsible for more than one system.	CA-2

Policy ID	DHS Policy Statements	Relevant Controls
2.1.7.c	The Security Control Assessor may take the lead for any or all remedial actions.	CA-7
2.1.7d	The Security Control Assessor provides an assessment of the severity of weaknesses or deficiencies in the information systems, and clarifies they prepare the final security assessment report containing the results and findings from the assessment but not making a risk determination.	CA-7

2.1.8 Information Systems Security Officer

An ISSO performs security actions for an information system. There is only one ISSO designated to a system, but multiple Alternate ISSOs may be designated to assist the ISSO.

While the ISSO performs security functions, the System Owner is always responsible for information system security.

See *DHS 4300A Sensitive Systems Handbook, Attachment C – Information Systems Security Officer (ISSO) Designation Letter.*

Policy ID	DHS Policy Statements	Relevant Controls
2.1.8.a	An ISSO shall be designated for every information system and serve as the point of contact (POC) for all security matters related to that system.	PL-1
2.1.8.b	An ISSO shall ensure the implementation and maintenance of security controls in accordance with the Security Plan (SP) and DHS policies.	PL-1
2.1.8.c	An ISSO may be a DHS employee or a contractor.	PL-1
2.1.8.d	An ISSO may be assigned to more than one system.	PL-1
2.1.8.e	ISSO duties shall not be assigned as collateral duties unless approved by the Component CISO.	PL-1
2.1.8.f	The ISSO shall have a clearance greater than or equal to the highest level of information contained on the system. The minimum clearance for an ISSO shall be Secret.	

2.2 Other Roles

Roles related to, but not directly responsible for, information system security are described in the following subsections.

2.2.1 Secretary of Homeland Security

The Secretary of Homeland Security is responsible for fulfilling the Department's mission, which includes ensuring that DHS information systems and their data are protected in

accordance with Congressional and Presidential directives. The Secretary's role with respect to information system security is to allocate adequate resources.

To that end, the Secretary:

- Ensures that DHS implements its Information Security Program throughout the life cycle of each DHS system
- Submits (1) the DHS CIO's assessment of the adequacy and effectiveness of the Department's information security procedures, practices, and FISMA compliance, (2) the results of an annual independent information security program evaluation performed by the DHS Office of the Inspector General (OIG), and (3) the Senior Agency Official for Privacy's (SAOP) annual assessment of the Department's privacy policies, procedures, and practices to the Director of OMB
- Provides information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the Department, and on information systems used or operated by the Department, or by a contractor or other organization on behalf of the Department
- Ensures that an information security program is developed, documented, and implemented to provide security for all systems, networks, and data that support the Department's operations
- Ensures that information security processes are integrated with strategic and operational planning processes to secure the Department's mission
- Ensures that senior agency officials within the Department are given the necessary authority to secure the operations and assets under their control
- Delegates authority to the CIO to ensure compliance with applicable information security requirements

2.2.2 Under Secretaries and Heads of DHS Components

The Under Secretaries and the heads of DHS Components are responsible for oversight of the Component information security program, including appointing CIOs. Persons filling this role allocate adequate resources to information systems for information system security.

Policy ID	DHS Policy Statements	Relevant Controls
2.2.2.a	The Under Secretaries of Homeland Security and Heads of Components shall ensure that information systems and their data are sufficiently protected.	PL-1

Under Secretaries and the Heads of DHS Components:

- Appoint CIOs
- Ensure that an Information Security Program is established and managed in accordance with DHS policy and implementation directives

- Ensure that the security of information systems is an integral part of the life cycle management process for all information systems developed and maintained within their Components
- Ensure that adequate funding for information security is provided for Component information systems and that adequate funding requirements are included for all information systems budgets
- Ensure that information system data are entered into the appropriate DHS Security Management Tools to support DHS information security oversight and FISMA reporting requirements
- Ensure that the requirements for an information security performance metrics program are implemented and the resulting data maintained and reported

2.2.3 DHS Chief Information Officer

The DHS CIO is the senior agency executive responsible for all DHS information systems and their security as well as for ensuring FISMA compliance.

Policy ID	DHS Policy Statements	Relevant Controls
2.2.3.a	The DHS CIO shall develop and maintain the DHS Information Security Program.	PL-1
2.2.3.b	The DHS CIO designates the DHS CISO.	PL-1

The DHS CIO:

- Oversees the development and maintenance of a Department-wide information security program
- Appoints a DHS employee in writing to serve as the DHS CISO
- Serves as the AO for DHS enterprise information systems. This responsibility may be delegated in writing as appropriate
- Participates in developing DHS performance plans, including descriptions of the time periods and budget, staffing, and training resources required to implement the Department-wide security program
- Ensures that all information systems acquisition documents, including existing contracts, include appropriate information security requirements and comply with DHS information security policies
- Ensures that DHS security programs integrate fully into the DHS enterprise architecture and capital planning and investment control processes
- Ensures that System Owners understand and appropriately address risks, including interconnectivity with other programs and systems outside their control
- Reviews and evaluates the DHS Information Security Program annually

- Ensures that an information security performance metrics program is developed, implemented, and funded
- Reports to the DHS Under Secretary for Management on matters relating to the security of DHS systems
- Ensures compliance with applicable information security requirements
- Heads an office with the mission and resources to assist in ensuring Component compliance with the DHS Information Security Program
- Coordinates and advocates resources for enterprise security solutions
- Leads the DHS Contingency Planning program

2.2.4 Component Chief Information Officer

The Component CIO is responsible for Component information systems and their security as well as for ensuring FISMA compliance within the Component.

Policy ID	DHS Policy Statements	Relevant Controls
2.2.4.a	The Component CIO shall develop and maintain the Component Information Security Program.	PL-1, PM-1

Component CIOs:

- Establish and oversee their Component information security programs
- Ensure that an AO has been appointed for all Component information systems and serve as the AO for any information system where an AO has not been appointed or where a vacancy exists
- Ensure that information security concerns are addressed by Component Configuration Control Boards, Enterprise Architecture Board (EAB), and Acquisition Review Board (ARB)/Investment Review Board (IRB)
- Ensure that an accurate information systems inventory is established and maintained
- Ensure that all information systems acquisition documents, including existing contracts, include appropriate information security requirements and comply with DHS information security policies
- Ensure that System Owners understand and appropriately address risks, including interconnectivity with other programs and systems outside their control
- Ensure that an information security performance metrics program is developed, implemented, and funded
- Advise the DHS CIO of any issues regarding infrastructure protection, vulnerabilities or issues that may cause public concern or loss of credibility
- Ensure that incidents are reported to the DHS EOC within reporting time requirements as defined in Attachment F, *Incident Response* of the *DHS Sensitive Systems Handbook*

- Work with the DHS CIO and Public Affairs Office in preparation for public release of security incident information. The DHS CIO, or designated representative, has sole responsibility for public release of security incident information.
- Ensure compliance with DHS information systems security policy
- Coordinate and advocate resources for information security enterprise solutions

The following Component CIOs shall appoint a CISO and ensure that the CISO has resources to assist with Component compliance with policy. CISOs shall be DHS employees.

- Customs and Border Protection
- Immigration and Customs Enforcement
- Transportation Security Administration
- United States Secret Service
- United States Coast Guard
- Federal Emergency Management Agency
- United States Citizenship and Immigration Services
- Federal Law Enforcement Training Center

All other Component CIOs:

- Ensure that Component ISSMs have been appointed and provide the resources and qualified personnel to ensure Component compliance with DHS security policy

2.2.5 DHS Chief Security Officer

The DHS Chief Security Officer (CSO) implements and manages the DHS Security Program for DHS facilities and personnel.

The CSO is a senior agency official who reports directly to the Deputy Secretary on all matters pertaining to facility and personnel security within the DHS.

Policy ID	DHS Policy Statements	Relevant Controls
2.2.5.a	DHS information systems that control physical access shall be approved to operate in accordance with this policy document, whether they connect to other DHS information systems or not.	CA-1
2.2.5.b	The DHS CSO shall be the AO for all systems automating or supporting physical access controls or shall appoint an AO for each of those systems.	CA-6

2.2.6 DHS Chief Privacy Officer

The DHS Chief Privacy Officer is the head of the DHS Privacy Office and oversees privacy activities throughout DHS.including creating and ensuring compliance with privacy policy. The DHS Chief Privacy Officer assists the Component Privacy Officers and Privacy Points of Contact (PPOC) with privacy policy compliance at the Component level.

The DHS Chief Privacy Officer implements and manages the DHS Privacy Program, including creating DHS privacy policy and ensuring compliance with privacy policy. The DHS Chief Privacy Officer is responsible for DHS privacy policy and its compliance. The DHS Chief Privacy Officer assists the Component Privacy Officers and PPOC with policy compliance at the Component level.

Policy ID	DHS Policy Statements	Relevant Controls
2.2.6.a	The Chief Privacy Officer shall review program and system Privacy Threshold Analyses (PTA), Privacy Impact Assessments (PIA), and System of Records Notices (SORN), providing approval as appropriate.	PL-1, PL-5

The Chief Privacy Officer, as the senior official:

- Oversees privacy incident management
- Responds to suspected or confirmed privacy incidents or incidents involving PII
- Coordinates with the DHS CIO, DHS CISO, the DHS EOC, and senior management regarding privacy incidents
- Convenes and chairs incident response teams, such as the Privacy Incident Response Team (PIRT) and the Core Management Group (CMG)
- Approves program and system PTAs, PIAs, and SORNs
- Designates Privacy Sensitive Systems based on validated PTAs. Privacy Sensitive Systems are those that maintain PII
- Provides Department-wide annual and refresher privacy training

2.2.7 DHS Chief Financial Officer

The DHS CFO implements and manages the DHS Financial Program, including oversight of DHS financial systems. The DHS CFO designates financial systems and oversees security control definitions for financial systems.

Policy ID	DHS Policy Statements	Relevant Controls
2.2.7.a	The DHS CFO shall be the AO for all financial systems managed at the DHS level.	CA-6
2.2.7.b	The Component CFO shall be the AO for all financial systems managed by the Component.	CA-6
2.2.7.c	The DHS CFO shall designate the financial systems that fall under the DHS CFO mandated policy statements.	CA-6

Policy ID	DHS Policy Statements	Relevant Controls
2.2.7.d	The DHS CFO shall publish a comprehensive list of designated financial systems during the fourth quarter of every fiscal year. (This list shall be referred to as the CFO Designated Systems List.)	CA-6

All systems on the CFO Designated Systems List are required to conform with the policies defined in Sections 3.5.1 and 3.15.

2.2.8 Program Managers

Program Managers ensure compliance with applicable Federal laws and DHS policy directives governing the security, operation, maintenance, and privacy protection of information systems, information, projects, and programs under their control.

Program Managers are responsible for program-level POA&Ms that may impact one or more systems.

Policy ID	DHS Policy Statements	Relevant Controls
2.2.8.a	Program Managers shall ensure that program POA&Ms are prepared and maintained.	CA-5, PM-4
2.2.8.b	Program Managers shall prioritize security weaknesses for mitigation.	CA-5
2.2.8.c	Program Managers shall provide copies of program POA&Ms to affected System Owners.	CA-5, PM-4
2.2.8.d	Program Managers shall ensure that POA&Ms address the following: ▪ known vulnerabilities in the information system ▪ the security categorization of the information system ▪ the specific weaknesses or deficiencies in the information system security controls ▪ the importance of the identified security control weakness or deficiencies ▪ the Component's proposed risk mitigation approach to address the identified weaknesses or deficiencies in the security controls the Component's rationale for accepting certain weaknesses or deficiencies in the security controls.	CA-5

2.2.9 System Owners

System Owners use information technology to help achieve the mission needs within their program area of responsibility. They are responsible for the successful operation of the information systems and programs within their program area and are ultimately accountable for their security. All systems require a System Owner designated in writing for proper administration of security.

Policy ID	DHS Policy Statements	Relevant Controls
2.2.9.a	System Owners shall ensure that each of their systems is deployed and operated in accordance with this policy document.	PL-1
2.2.9.b	System Owners shall ensure that an ISSO is designated in writing for each information system under their purview.	PL-1
2.2.9.c	There shall be only one System Owner designated for each DHS system.	PL-1
2.2.9.d	The Information System Owner shall information security compliance, development and maintenance of security plans, user security training, notifying officials of the need for security authorization and need to resource.	CA-2
2.2.9.e	System Owners shall ensure development of a POA&M to address weaknesses and deficiencies in the information system and its environment of operation which remain after Security Authorization.	CA-2

2.2.10 Common Control Provider

The Common Control Provider is an organizational official responsible for the planning, development, implementation, assessment, authorization, and maintenance of common controls.

2.2.10.a	The Common Control Provider shall document all common controls and submit them to the AO and DHS CISO.	PM-1
2.2.10.b	The Common Control Provider ensures that required assessments of common controls are carried out by qualified assessors with the appropriate level of independence.	PM-1
2.2.10.c	The Common Control Provider documents assessment findings in a security assessment report.	PM-1
2.2.10.d	The Common Control Provider ensures that POA&Ms are developed for all controls having weaknesses or deficiencies.	PM-4
2.2.10.e	The Common Control Provider shall make available security plans, Security Assessment Reports (SARs), and POA&Ms for common controls to information system owners inheriting those controls after the information is reviewed and approved by a senior official.	PM-1, PM-4

2.2.11 DHS Employees, Contractors, and Others Working on Behalf of DHS

DHS employees, contractors, and others working on behalf of the DHS or its agencies shall follow the appropriate set(s) of rules of behavior.

Policy ID	DHS Policy Statements	Relevant Controls
2.2.11.a	DHS users shall follow prescribed rules of behavior.	PL-4

3.0 MANAGEMENT POLICIES

3.1 Basic Requirements

Basic security management principles must be followed in order to ensure the security of DHS information resources. These principles are applicable throughout the Department and form the cornerstone of the DHS Information Security Program.

Component CISOs/ISSMs shall submit all security reports concerning DHS systems to the Component senior official or designated representative. Component CISOs/ISSMs shall interpret and manage DHS security policies and procedures to meet Federal, Departmental, and Component requirements. They shall also answer data queries from the DHS CISO and develop and manage information security guidance and procedures unique to Component requirements.

ISSOs are the primary points of contact for the information systems assigned to them. They develop and maintain Security Plans (SP) and are responsible for overall system security.

Policy ID	DHS Policy Statements	Relevant Controls
3.1.a	Every DHS computing resource (e.g., desktops, laptops, servers, portable electronic devices) shall be individually accounted for as part of a recognized information system.	CM-8
3.1.b	The Component CIO, in cooperation with each Component senior official, shall be responsible for ensuring that every DHS computing resource is identified as an information system or as a part of an information system (major application or general support system).	CM-8
3.1.c	The System Owner or designee shall develop and maintain an SP for each information system. Component AOs shall review and approve SPs.	PL-2
3.1.d	An ISSO shall be designated for every information system and serve as the point of contact (POC) for all security matters related to that system.	PL-1
3.1.e	Component Information Security Programs shall be structured to support DHS and applicable FISMA, OMB, and other Federal requirements.	PL-1
3.1.f	Information security reports regarding DHS systems shall be submitted to the Component senior official or designated representative.	---
3.1.g	Component CISOs/ISSMs shall ensure that their information systems comply with the DHS Enterprise Architecture (EA) Technical Reference model (TRM) and Security Architecture (SA) or maintain a waiver, approved by the DHS CIO/CISO.	PL-1
3.1.h	The DHS CISO shall issue Department-wide information security policy, guidance, and architecture requirements for all DHS systems.	CM-2, CM-6
3.1.i	Component CISOs shall implement DHS information security policies, procedures, and control techniques to address all applicable requirements.	PL-1

Policy ID	DHS Policy Statements	Relevant Controls
3.1.j	Component CISOs shall develop and manage information security guidance and procedures unique to Component requirements.	PL-1

3.2 Capital Planning and Investment Control

Information security is a business driver and any risks found through security testing are ultimately business risks. Information security personnel should be involved, to the maximum extent possible, in all aspects of the acquisition process, including drafting contracts, and procurement documents. Directive 102-01, Acquisition Management Directive and MD 4200.1, IT Capital Planning and Investment Control (CPIC), and Portfolio Management provide additional information on these requirements.

Policy ID	DHS Policy Statements	Relevant Controls
3.2.a	System Owners shall include information security requirements in their CPIC business cases for the current budget year and for the Future Years Homeland Security Program (FYHSP) for each DHS system.	PM-3, PM-11, SA-1
3.2.b	System Owners or AOs shall ensure that information security requirements and POA&Ms are adequately funded, resourced and documented in accordance with current OMB budgetary guidance.	PM-3, PM-4, SA-2
3.2.c	Component IRBs/ARBs shall not approve any capital investment in which the information security requirements are not adequately defined and funded.	PM-3, SA-2
3.2.d	The DHS CISO shall perform security reviews for planned information system acquisitions over $2.5 million and additional selected cases.	SA-1
3.2.e	Components shall ensure that information security requirements as described within this policy document are included in the acquisition of all DHS systems and services used to input, process, store, display, or transmit sensitive information.	SA-4
3.2.f	Procurement authorities throughout the Department shall ensure that Homeland Security Acquisition Regulation (HSAR) provisions are fully enforced.	SA-1, SA-4
3.2.g	Procurements for services and products involving facility or system access control shall be in accordance with the DHS guidance regarding HSPD-12 implementation.	

3.3 Contractors and Outsourced Operations

Policy ID	DHS Policy Statements	Relevant Controls
3.3.a	All statements of work and contract vehicles shall identify and document the specific security requirements for information system services and operations required of the contractor.	SA-4
3.3.b	Contractor information system services and operations shall adhere to all applicable DHS information security policies.	SA-9
3.3.c	Requirements shall address how sensitive information is to be handled and protected at contractor sites, including any information stored, processed, or transmitted using contractor information systems. Requirements shall also include requirements for personnel background investigations and clearances, and facility security.	SA-9
3.3.d	Statements of work and contracts shall include a provision stating that, upon the end of the contract, the contractor shall return all information and information resources provided during the life of the contract and certify that all DHS information has been purged from any contractor-owned system used to process DHS information.	SA-4
3.3.e	Components shall conduct reviews to ensure that the information security requirements are included within the contract language and are implemented and enforced.	SA-1
3.3.f	Security deficiencies in any outsourced operation shall require creation of a program-level POA&M.	SA-9, PM-4

3.4 Performance Measures and Metrics

Policy ID	DHS Policy Statements	Relevant Controls
3.4.a	The DHS CISO shall define performance measures to evaluate the effectiveness of the DHS information security program.	---
3.4.b	Components shall provide OMB FISMA data at least monthly to the DHS Compliance Officer.	---
3.4.c	The DHS CISO shall report annually to the Secretary on the effectiveness of the DHS information security program, including the progress of remedial actions.	---
3.4.d	Components shall utilize the automated tool directed for use by the DHS CISO for Performance Plan reporting.	---

Policy ID	DHS Policy Statements	Relevant Controls
3.4.e	The DHS CISO shall collect OMB FISMA data from Components at least quarterly and provide FISMA reports to OMB.	---

3.5 Continuity Planning for Critical DHS Assets

The Continuity Planning for Critical DHS Assets Program is vital to the success of the DHS Information Security Program. The Business Impact Assessment (BIA), which is part of the Contingency, is essential in the identification of critical DHS assets. Once critical systems are identified, continuity planning shall address the following two complementary but different elements:

- Continuity of Operations Planning (COOP)
- Contingency Planning (CP)

3.5.1 Continuity of Operations Planning

Policy ID	DHS Policy Statements	Relevant Controls
3.5.1.a	When available, a DHS-wide process for continuity planning shall be used in order to ensure continuity of operations under all circumstances.	CP-2
3.5.1.b	Components shall develop, test, implement, and maintain comprehensive Continuity of Operations Plans (COOP) to ensure the continuity and recovery of essential DHS functionality.	CP-2, CP-4
3.5.1.c	All CISOs/ISSMs shall ensure that all COOPs under their purview are tested and exercised annually.	CP-4
3.5.1.d	All CFO Designated Systems requiring high availability shall be identified in COOP plans and exercises.	CP-1
3.5.1.e	All personnel involved in COOP efforts shall be identified and trained in the procedures and logistics of COOP development and implementation.	AT-3, CP-3
3.5.1.f	To ensure that accounts can be created in the absence of the usual account approval authority, systems that are part of the Critical DHS Assets Program shall have provisions to allow a Component CISO/ISSM or Component CIO to approve new user accounts as part of a COOP scenario.	AC-2
3.5.1.g	Each Component shall compile and maintain a list of mission-critical information systems in support of COOP.	CM-8, CP-1
3.5.1.h	The DHS and Component CISOs/ISSMs shall ensure preparation and maintenance of plans and procedures to provide continuity of operations for information systems.	CP-1

Policy ID	DHS Policy Statements	Relevant Controls
3.5.1.i	DHS information systems that are part of the DHS Continuity Planning for Critical DHS Assets Program shall be provided requirements for system-level contingency planning by a Component Contingency Planning Program Office or by a DHS Contingency Planning Program Office.	---

3.5.2 Contingency Planning

Policy ID	DHS Policy Statements	Relevant Controls
3.5.2.a	The DHS CIO shall provide guidance, direction, and authority for a standard DHS-wide process for contingency planning for all DHS Components.	CP-1
3.5.2.b	System Owners shall develop and document information system Contingency Plans (CPs) for their programs, manage plan changes, and distribute copies of the plan to key contingency personnel. Component CIOs shall review and approve Component-level information system CPs.	CP-1, CP-2
3.5.2.c	Components shall ensure implementation of backup policy and procedures for every Component information system.	CP-9
3.5.2.d	The DHS CIO shall ensure that each system has contingency capabilities commensurate with the **availability** security objective. The minimum contingency capabilities for each impact level follow: **High** – System functions and information have a high priority for recovery after a short period of loss. **Moderate** – System functions and information have a moderate priority for recovery after a moderate period of loss. **Low** – System functions and information have a low priority for recovery after prolonged loss.	CP-1
3.5.2.e	CPs shall be developed and maintained by all DHS Components in accordance with the requirements for the FIPS 199 potential impact level for the **availability** security objective. These plans shall be based on three essential phases: Activation/Notification, Recovery, and Reconstitution. Components shall review the CP for the information system at least annually and revise the plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.	CP-1, CP-2
3.5.2.f	The DHS CIO shall ensure that CP testing is performed in accordance with the **availability** security objective. The minimum contingency testing for each impact level follows: **High** – System recovery roles, responsibilities, procedures, and logistics in the CP shall be used to recover from a simulated contingency event at the alternate processing site within a year prior to accreditation. The system recovery procedures in the CP shall be used to simulate system recovery in a test facility at least annually.	CP-4, CP-7

Policy ID	DHS Policy Statements	Relevant Controls
	Moderate – The CP shall be tested at least annually by reviewing and coordinating with organizational elements responsible for plans within the CP. This is achieved by performing a walk-through/tabletop exercise. **Low** – CP contact information shall be verified at least annually.	
3.5.2.g	The DHS CIO shall ensure that contingency training is performed in accordance with the **availability** security objective. The minimum contingency planning for each impact level follows: **High** – All personnel involved in contingency planning efforts shall be identified and trained in their contingency planning and implementation roles, responsibilities, procedures, and logistics. This training shall incorporate simulated events. Refresher training shall be provided at least annually. **Moderate** – All system personnel involved in contingency planning efforts shall be trained. Refresher training shall be provided at least annually. **Low** – There is no training requirement.	CP-3
3.5.2.h	Components shall coordinate as appropriate CP testing and/or exercises with COOP related plans for systems with moderate and high availability FIPS-199 categorization.	CP-4

3.6 System Engineering Life Cycle

Directive 102-01, Acquisition Management Directive, Appendix B, contains the DHS Systems Engineering Life Cycle (SELC).

Policy ID	DHS Policy Statements	Relevant Controls
3.6.a	Components shall ensure that system security is integrated into all phases of the Systems Engineering Life Cycle (SELC).	SA-3
3.6.b	Components shall ensure that security requirements for sensitive information systems are incorporated into life-cycle documentation.	SA-3
3.6.c	The Program Manager shall review, approve, and sign all custom-developed code prior to deployment into production environments. The Program Manager may delegate this authority to another DHS employee in writing. This authority shall not be delegated to contractor personnel.	RA-5

3.7 Configuration Management

Configuration management (CM) relates to managing the configuration of all hardware and software elements within information systems and networks. CM within DHS consists of a multi-layered structure – policy, procedures, processes, and compliance monitoring. Each Component shall utilize appropriate levels of configuration management.

CM applies to all systems, subsystems, and components of the DHS infrastructure, thereby ensuing implementation, and continuing life-cycle maintenance. CM begins with baselining of

requirements documentation and ends with decommissioning of items no longer used for production or support.

The CM discipline applies to hardware, including power systems, software, firmware, documentation, test and support equipment, and spares. A Change Management Process ensures that documentation associated with an approved change to a DHS system is updated to reflect the appropriate baseline, including an analysis of any potential security implications. The initial configuration must be documented in detail and all subsequent changes must be controlled through a complete and robust CM process. Configuration management has security implications in three areas:

- Ensuring that the configuration of subordinate information system elements are consistent with the Security Authorization Process requirements of the parent system
- Ensuring that any subsequent changes, including an analysis of any potential security implications, are approved
- Ensuring that all recommended and approved security patches are properly installed

DHS Sensitive Systems Handbook, Enclosure 1, includes the DHS Secure Baseline Configuration Guides.

Policy ID	DHS Policy Statements	Relevant Controls
3.7.a	Components shall develop and maintain a configuration management plan (CMP) for each information system as part of its SP. All DHS systems shall be under the oversight of a Configuration Management responsible officer.	CM-1, CM-9
3.7.b	Components shall establish, implement, and enforce configuration management controls on all information systems and networks and address significant deficiencies as part of a POA&M.	CA-5, CM-3, PM-4
3.7.c	Information security patches shall be installed in accordance with configuration management plans and within the timeframe or direction stated within the Information Security Vulnerability Management (ISVM) message published by the DHS EOC.	SI-2
3.7.d	System Owners shall document the initial system configuration in detail and control all subsequent changes in accordance with the configuration management process.	CM-2, CM-3, CM-9
3.7.e	Workstations shall be configured in accordance with DHS guidance on the U.S Government Configuration Baseline (USGCB) (formerly known as the Federal Desktop Core Configuration [FDCC]). Configuration shall include installation of the DHS Common Policy Object identifier (OID), Common Policy Framework Root CA certificate, and the DHS Principal CA certificate.	CM-2, CM-6, CM-9
3.7.f	Components shall monitor USGCB (or DHS-approved USGCB variant) compliance using a NIST-validated Security Content Automation Protocol (SCAP) tool.	

Policy ID	DHS Policy Statements	Relevant Controls
3.7.g	The System Owner shall request an exception for information systems that use operating systems or applications that are not hardened or do not follow configuration guidance identified in DHS Sensitive Systems Handbook, Enclosure 1, DHS Secure Baseline Configuration Guides. Requests shall include a proposed alternative secure configuration.	CM-2, CM-6
3.7.h	Components shall ensure that CM processes under their purview include and consider the results of a security impact analysis when considering proposed changes.	CM-4

3.8 Risk Management

Risk management is a process that allows System Owners to balance the operational and economic costs of protective measures to achieve gains in mission capability by protecting the information systems and data that support their organization's missions.

Policy ID	DHS Policy Statements	Relevant Controls
3.8.a	Components shall establish a risk management program in accordance with NIST SP 800-30, *Risk Management Guide for Information Technology Systems* and other applicable Federal guidelines.	RA-1
3.8.b	Component CISOs/ISSMs shall ensure that a risk assessment is conducted whenever high impact weaknesses are identified, or every three (3) years or whenever modifications are made to sensitive information systems, or to their physical environments, interfaces, or user community. The risk assessment shall consider the effects of the modifications on the operational risk profile of the information system. SPs shall be updated and re-certification conducted if warranted by the results of the risk assessment.	RA-3
3.8.c	Component CISOs/ISSMs shall establish an independent Component-wide Security Authorization program to ensure a consistent approach to testing the effectiveness of controls.	RA-1
3.8.d	Risk Executives shall review recommendations for risk determinations and risk acceptability and may recommend changes to the AO and appropriate CIO.	RA-3
3.8.e	Component SOCs shall deploy a Component-wide network scanning program.	RA-5
3.8.f	Special rules apply to CFO Designated Systems. See Section 3.15 for additional information.	---

3.9 Security Authoziation and Security Assessments

DHS periodically assesses the selection of security controls to determine their continued effectiveness in providing an appropriate level of protection.

The DHS *Security Authorization Process Guide* describes detailed processes governing *Security Authorization Process* and system risk assessment.

Detailed information for creating and managing POA&Ms is published in DHS 4300A *Sensitive Systems Handbook, Attachment H – Plan of Action and Milestones (POA&M) Process Guide*.

Policy ID	DHS Policy Statements	Relevant Controls
3.9.a	Components shall assign an impact level (high, moderate, low) to each security objective (confidentiality, integrity, and availability) for each DHS information system. Components shall apply NIST SP 800-53 controls as tailored in the DHS 4300A, *Sensitive Systems Handbook, Attachment M* specific to the security objective at the determined impact level.	PM-10, RA-2
3.9.b	Components shall implement NIST SP 800-53 security controls, using the FIPS Pub 200, *Minimum Security Requirements for Federal Information and Information Systems* methodology, based on the FIPS 199 impact level established for each separate security objective (confidentiality, integrity, availability).	---
3.9.c	Recommend that Components pursue type *Security Authorization Process* for information resources that are under the same direct management control; have the same function or mission objective, operating characteristics, security needs, and that reside in the same general operating environment, or in the case of a distributed system, reside in various locations with similar operating environments. Type *Security Authorization Process* shall consist of a master *Security Authorization Process* package describing the common controls implemented across sites and site-specific controls and unique requirements that have been implemented at the individual sites.	---
3.9.d	The AO for a system shall be identified in TrustedAgent FISMA. The Component CIO shall serve as the AO whenever the System Owner or an appropriate program official has not been named as the AO.	---
3.9.e	Component CISOs shall ensure that all information systems are formally assessed through a comprehensive evaluation of their management, operational, and technical security controls.	CA-2, PM-10
3.9.f	The assessment, made as part of and in support of the accreditation process, shall determine the extent to which a particular design and implementation plan meets the DHS required set of security controls.	PM-10
3.9.g	Component CISOs/ISSMs shall ensure that a risk assessment is conducted whenever any modifications are made to sensitive information systems, networks, or to their physical environments, interfaces, or user community. SPs shall be updated and re-authorized conducted if warranted.	PM-9, RA-3

Policy ID	DHS Policy Statements	Relevant Controls
3.9.h	Components shall accredit systems at initial operating capability and every three (3) years thereafter, or whenever a major change occurs, whichever occurs first. An ATO of six (6) months or less shall receive an ATO accreditation period waiver from the DHS CISO before submission to the AO for a final accreditation decision.	CA-6, PM-10
3.9.i	AOs may grant an Interim Authorization to Operate (IATO) for systems that are undergoing development testing or are in a prototype phase of development. A system shall be assessed and authorized in an ATO letter prior to passing the Key Decision Point 3 milestone in the SELC. IATOs shall not be used for operational systems. The AO may grant an IATO for a maximum period of 6 (six) months and may grant 1 (one) 6 (six) month extension. Systems under an IATO shall not process sensitive information but may attach to system networks for testing.	PL-1, PM-10
3.9.j	If the system is not fully accredited and has not received a full ATO by the end of the second and final IATO, the system shall not be deployed as an operational system.	PL-1, PM-10
3.9.k	As a result of Office of Inspector General (OIG) auditing experience, Components shall request concurrence from the DHS CISO for all accreditations for 6 (six) months or less.	---
3.9.l	The DHS CISO shall specify tools, techniques, and methodologies used to certify and accredit DHS information systems, report and manage FISMA data, and document and maintain POA&Ms.	CA-1, PM-4
3.9.m	Currently, all DHS systems shall be accredited using the automated tools, TAF and RMS, which have been approved by the DHS CISO.	CA-1, CA-2, PM-10
3.9.n	The DHS CISO shall maintain a repository for all *Security Authorization Process* documentation and modifications.	CA-1
3.9.o	Component CISOs shall establish processes to ensure consistent *Security Authorization Process* processing across all Component systems.	CA-1, PM-10
3.9.p	System Owners shall use the POA&M process to manage vulnerabilities, correct deficiencies in security controls, and remediate weaknesses in SPs.	CA-5, PM-4
3.9.q	The AO shall formally assume responsibility for operating an information system at an acceptable level of risk. System operation with sensitive information is prohibited without an ATO.	CA-6, PM-10
3.9.r	ATOs shall only be provided for systems that fully comply with policy or have been granted appropriate exceptions or waivers.	CA-6, PM-10

Policy ID	DHS Policy Statements	Relevant Controls
3.9.s	Artifacts in support of *new* ATOs shall not be older than 13 months. Older artifacts remain valid during the life of a current ATO.	---
3.9.t	The DHS CIO may revoke any ATO of any DHS information system.	CA-6
3.9.u	The Component CIO may revoke the ATO of any Component-level information system.	CA-6
3.9.v	Components shall assign a common control provider to share controls between systems (e.g., at hosting centers). The authorization package of those common controls must be shared with those operating under them.	

3.10 Information Security Review and Assistance

Policy ID	DHS Policy Statements	Relevant Controls
3.10.a	Components shall submit their information security policies to the DHS CISO for review.	PL-1
3.10.b	Components shall establish an information system security review and assistance program within their respective security organization in order to provide System Owners with expert review of programs, assist in identifying deficiencies, and provide recommendations for bringing systems into compliance.	CA-7, PL-1, PM-10
3.10.c	Components shall conduct their reviews in accordance with FIPS 200/NIST SP 800-53, for specification of security controls. NIST SP 800-53A shall be used for assessing the effectiveness of security controls and for quarterly and annual FISMA reporting.	CA-7, PL-1
3.10.d	The DHS CISO shall conduct information security review and assistance visits across the Department in order to monitor the effectiveness of Component security programs.	CA-2

3.11 Security Working Groups and Forums

Working groups and other forums representing various functional areas convene on a regular basis.

3.11.1 CISO Council

The CISO Council is the management team responsible for developing and implementing the DHS Information Security Program. The Council is responsible for implementing a security program that meets DHS mission requirements, and reviewing specific topic areas assigned by the DHS CIO or the DHS CISO.

The CISO Council is also responsible for establishing and implementing significant security responsibilities, promoting communications between security programs, implementing information systems security acquisition requirements, and developing security best practices within all enterprise and Component information security programs.

Policy ID	DHS Policy Statements	Relevant Controls
3.11.1.a	Component CISOs shall actively participate in the CISO Council.	PL-1, PM-11
3.11.1.b	Members shall ensure that the DHS CISO is kept apprised of all pertinent matters involving the security of information systems.	PL-1, PM-11
3.11.1.c	Members shall ensure that security-related decisions and information, including updates to the 4300 series of security publications, are distributed to the ISSOs and other appropriate persons.	PL-1, PM-11

Note: Periodically, the CISO Council shall be convened to include Component ISSMs.

3.11.2 DHS Information Security Training Working Group

The DHS Information Security Training Working Group is established to promote collaboration on information security training efforts throughout the Department and to share information on Component-developed training activities, methods, and tools, thereby reducing costs and avoiding duplication of effort. The Information Security Training Working Group is chaired by the DHS Program Director for Information Security Training.

Policy ID	DHS Policy Statements	Relevant Controls
3.11.2.a	Components shall appoint a representative to the DHS Information Security Training Working Group.	---
3.11.2.b	Members shall actively participate in the DHS Information Security Training Working Group.	---
3.11.2.c	Components shall abide by the security training requirements listed in the Information Security Awareness, Training, and Education section of this policy.	---

3.12 Information Security Policy Violation and Disciplinary Action

Individual accountability is a cornerstone of an effective security policy. Component Heads are responsible for taking corrective actions whenever security incidents and violations occur and for holding personnel accountable for intentional transgressions. Each Component must determine how to best address each individual case.

Policy ID	DHS Policy Statements	Relevant Controls
3.12.a	Information security-related violations are addressed in the *Standards of Ethical Conduct for Employees of the Executive Branch* and DHS employees may be subject to disciplinary action for failure to comply with DHS security policy, whether or not the failure results in criminal prosecution.	PS-8
3.12.b	Non-DHS Federal employees, contractors, or others working on behalf of DHS who fail to comply with Department security policies are subject to having their access to DHS systems and facilities terminated, whether or not the failure results in criminal prosecution.	PS-8
3.12.c	Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions.	PS-8

3.13 Required Reporting

FISMA requires that the status of the DHS Information Security Program be reported to the OMB on a recurring basis.

Policy ID	DHS Policy Statements	Relevant Controls
3.13.a	Components shall collect and submit quarterly and annual information security program status data as required by FISMA.	CA-2
3.13.b	Components shall utilize the automated tool approved for use by the DHS CISO.	CA-2

3.14 Privacy and Data Security

The DHS Privacy Office is responsible for privacy compliance across the Department, including assuring that technologies used by the Department sustain and do not erode privacy protections relating to the use of personal and Department information. The DHS Chief Privacy Officer has exclusive jurisdiction over the development of policy relating to personally identifiable information (PII). Questions concerning privacy-related policy should be directed to the Component Privacy Office or PPOC. If the Component does not have a Privacy Office or PPOC, then please contact the DHS Privacy Office (privacy@dhs.gov; 703-235-0780) or refer to the DHS Chief Privacy Officer web page for additional information.

3.14.1 Personally Identifiable Information

Various regulations place restrictions on the Government's collection, use, maintenance, and release of information about individuals. Regulations require agencies to protect PII, which is any information that permits the identity of an individual to be directly or indirectly inferred, including any information which is linked or linkable to that individual regardless of whether or not the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.

Sensitive PII is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Examples of Sensitive PII include Social Security numbers, alien numbers (A-number), medical information, and criminal history. The sensitivity of this data requires that stricter handling guidelines be applied. For more information on handling Sensitive PII see: *Handbook for Safeguarding Sensitive Personally Identifiable Information at the Department of Homeland Security.*

Additional PII and Sensitive PII-related policies are included in the following sections of the DHS 4300A *Sensitive Systems Handbook.*

- Section 3.9, Security Authorization Process, and Security Assessments – For Privacy Sensitive Systems, the confidentiality security objective shall be assigned an impact level of at least moderate.
- Section 4.8.2, Laptop Computers and Other Mobile Computing Devices – All information stored on any laptop computer or other mobile computing device is to be encrypted using mechanisms that comply with Section 5.5, Encryption, of this policy.
- Section 5.2.2, Automatic Session Termination – Sessions on workstations and on laptop computers and other mobile computing devices are to be terminated after twenty (20) minutes of inactivity.
- Section 5.3, Auditing – DHS defines computer-readable data extracts as data removed from any accredited system where the process is not covered by the SP and computer-readable data extracts are stored on hard drives, including desk top and laptop computers, floppy disks, compact discs (CDs), digital video disks (DVDs), USB drives, memory cards, and any other media that may be read or copied electronically.
- Section 5.4.1, Remote Access and Dial-in – Remote access of PII must be approved by the AO. Strong authentication via virtual private network (VPN) or equivalent encryption (e.g., https) and two-factor authentication is required. DHS has an immediate goal that remote access should only be allowed with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access. Restrictions are placed on the downloading and remote storage of PII accessed remotely, as noted below in the DHS Policy.

The DHS Privacy Office works with Component Privacy Officers, PPOCs, Program Managers, System Owners, and information systems security personnel to ensure that sound privacy practices and controls are integrated into the Department's operations. The DHS Privacy Office implements three types of documents for managing privacy practices and controls for information systems:

- A PTA provides a high level description of an information system including the information it contains and how it is used. The PTA is used to determine and document whether or not a PIA and/or SORN are required.
- A PIA is a publicly released assessment of the privacy impact of an information system and includes an analysis of the PII that is collected, stored, and shared.
- A SORN describes the categories of records within a system of records and describes the routine uses of the data and how individuals can gain access to records and correct errors.

To promote privacy compliance within the Department, the Office has published official Department guidance regarding the requirements and content for PTAs, PIAs, and SORNs. Privacy Compliance Guidance can be found on the DHS Privacy Office website at www.dhs.gov/privacy.

3.14.2 Privacy Threshold Analyses

The PTA provides a high-level description of the system, including the information it contains and how it is used. PTAs are required whenever a new information system is being developed or an existing system is significantly modified. System Owners and Program Managers are responsible for writing the PTA as part of the system development lifecycle process. The Component Privacy Officer or PPOC reviews the PTA and forwards it to the DHS Privacy Office, who determines whether a PIA and/or SORN are required. PTA artifacts expire after three (3) years. DHS MD 0470.2 defines the PTA requirements.

Policy ID	DHS Policy Statements	Relevant Controls
3.14.2.a	A PTA shall be conducted as part of new information system development or whenever an existing system is significantly modified. PTA artifacts expire after three (3) years and a new PTA must be submitted.	PL-5
3.14.2.b	A PTA shall be conducted whenever an information system undergoes security authorization.	---
3.14.2.c	The DHS Chief Privacy Officer shall evaluate the PTA and determine if it is a Privacy Sensitive System and if the system requires a PIA and SORN.	PL-5
3.14.2.d	Information systems shall not be designated operational until the DHS Privacy Office approves the PTA.	PL-5
3.14.2.e	For Privacy Sensitive Systems, the **confidentiality** security objective shall be assigned an impact level of moderate or higher.	RA-2

3.14.3 Privacy Impact Assessments

A PIA is a publicly released assessment of the privacy impact of an information system and includes an analysis of the PII that is collected, stored, and shared. PIAs are required (as determined by the PTA) whenever a new information system is being developed or an existing system is significantly modified. PIAs are the responsibility of the System Owner and the Program Manager as part of the SELC process. OMB Memorandum M-03-22, DHS MD 0470.1, and the *Official DHS Privacy Impact Assessment Guidance* discuss the requirements for conducting PIAs at DHS.

Policy ID	DHS Policy Statements	Relevant Controls
3.14.3.a	PIAs are required (as determined by the PTA) as part of new information system development or whenever an existing system is significantly modified.	PL-5
3.14.3.b	Information systems that the DHS Privacy Office has determined require a PIA (as determined by the PTA) shall not be designated operational until the DHS Privacy Office approves the PIA for that system.	PL-5

3.14.4 System of Records Notices

The Privacy Act of 1974 requires a SORN when PII is maintained by a Federal agency in a system of records and the PII is retrieved by a personal identifier. A system of records is "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual" 5 U.S.C.§552a (a)(5). The SORN describes the categories of records and individuals in the system of record; the routine uses of the data; how individuals can gain access to records pertaining to them and correct errors. The term "system of records" is not synonymous with an information system and can include paper as well as electronic records. SORNs can be written to cover the records in a single group of records or a single information system or they can be written to cover multiple groups of records or multiple information systems.

Information systems that are considered a system of record may not be designated operational until a SORN has been published in the *Federal Register* for thirty days. The Office of Management and Budget, specifically *Privacy Act Implementation, Guidelines and Responsibilities*, July 9, 1975, and *Circular A-130* including *Appendix I*, DHS MD 0470.2, and *Official DHS Guidance on System of Records and System of Records Notices* are the benchmark references when developing SORNs.

OMB requires each SORN to be reviewed every two (2) years to ensure that it accurately describes the system of records. This process is called the Biennial SORN Review Process. The DHS Privacy Office works with Components to ensure that SORN reviews are conducted every two (2) years following publication in the Federal Register.

Policy ID	DHS Policy Statements	Relevant Controls
3.14.4.a	A SORN is required when PII is maintained by a Federal agency in a system of records where information about an individual is retrieved by a unique personal identifier.	---
3.14.4.b	Information systems containing PII shall not be designated operational until a SORN has been published in the Federal Register for thirty (30) days.	CA-6
3.14.4.c	Components shall review and republish SORNs every two (2) years as required by OMB A-130.	

3.14.5 Protecting Privacy Sensitive Systems

OMB M-06-16, *Protection of Sensitive Agency Information* requires that agencies protect PII that is physically removed from Department locations or is accessed remotely. Physical removal includes both removable media as well as media within mobile devices (i.e., laptop hard drive). Please refer to the following documents for additional information and policies on protecting PII and Sensitive PII at DHS:

- *Handbook for Safeguarding Sensitive Personally Identifiable Information at the Department of Homeland Security*:
- *DHS* 4300 A, Sensitive System Handbook, Attachment S, *Compliance Framework for Privacy Sensitive Systems*; and
- *DHS Policy and Procedures for Managing Computer-Readable Extracts Containing Sensitive PII.*

In addition, see Section 5.3 for PII auditing requirements and Section 5.4.1 for remote access requirements.

Policy ID	DHS Policy Statements	Relevant Controls
3.14.5.a	PII and Sensitive PII removed from a DHS facility on removable media, such as CDs, DVDs, laptops, PDAs, shall be encrypted, unless the information is being sent to the individual as part of a Privacy Act or Freedom of Information Act (FOIA) request.	MP-5 SC-13
3.14.5.b	If PII and Sensitive PII can be physically removed from an information system (e.g., printouts, CDs), the Security Plan (SP) shall document the specific procedures, training, and accountability measures in place to ensure remote use of the data does not bypass the protections provided by the encryption.	MP-5
3.14.5.c	Systems that, as part of routine business, remove Sensitive PII in the form of a Computer-Readable Extract (CRE), e.g., routine system-to-system transmissions of data (routine CREs) shall address associated risks in the SP.	MP-5
3.14.5.d	Sensitive PII contained within a non-routine or ad hoc CRE (e.g., CREs not included within the boundaries of a source system's security plan) shall not be removed, physically or otherwise, from a DHS facility without written authorization from the Data Owner responsible for ensuring that the disclosure of the CRE data is lawful and in compliance with this and applicable DHS privacy and security policies.	---
3.14.5.e	All ad hoc CREs must be documented, tracked, and validated every ninety (90) days after their creation to ensure that their continued authorized use is still required or that they have been appropriately destroyed or erased.	---

Policy ID	DHS Policy Statements	Relevant Controls
3.14.5.f	Ad hoc CREs shall be destroyed or erased within ninety (90) days unless the information included in the extracts is required beyond that period. Permanent erasure of the extracts or the need for continued use of the data shall be documented by the Data Owner and audited periodically by the Component Privacy Officer or PPOC.	---

3.14.6 Privacy Incident Reporting

The DHS Privacy Office is responsible for implementing the Department's privacy incident response program based on requirements outlined in OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007 (M-07-16). Through close collaboration, the DHS Chief Privacy Officer, the DHS CIO, the DHS CISO, the DHS EOC, and Components must ensure that all DHS privacy and computer security incidents are identified, reported, and appropriately responded to, in order to mitigate harm to DHS-maintained assets, information, and personnel. Incidents involving (or that may involve) PII are subject to strict reporting standards and timelines.

Policy ID	DHS Policy Statements	Relevant Controls
3.14.6.a	Any Component discovering a suspected or confirmed privacy incident shall coordinate with the Component Privacy Officer or PPOC and Component CISO/ISSM to evaluate and subsequently report the incident to the DHS EOC immediately upon discovery. The DHS EOC will then transmit the report to the US-CERT within one (1) hour.	IR-4
3.14.6.b	The Component Privacy Officer or PPOC, in cooperation with the Component CISO/ISSM, shall jointly evaluate the incident, but the Component CISO/ISSM is responsible for reporting the incident to the Component SOC/ Computer Security Incident Response Capability (CSIRC) (or directly to the DHS EOC/CSIRC if the Component does not have its own SOC/CSIRC).	IR-4
3.14.6.c	For Components without Privacy Officers or PPOCs, the Component CISO/ISSM shall report *all* types of privacy incidents, whether or not they involve information resources. This unitary reporting process shall remain in effect until each Component has a Privacy Officer or PPOC who can fulfill the reporting duties.	IR-6
3.14.6.d	DHS personnel shall also report suspected or confirmed privacy incidents or incidents involving PII to their Program Manager immediately upon discovery/detection, regardless of the manner in which it might have occurred.	IR-6
3.14.6.e	Components shall follow the *DHS Privacy Incident Handling Guide*.	---

3.14.7 E-Authentication

Identity verification or authentication (e-authentication) is needed to ensure that online Government services are secure and that individual privacy is protected. Each DHS system must be evaluated to determine whether e-authentication requirements apply. Only federated identity providers approved through the Federal CIO Council's Identity, Credentialing, and Access Management's (ICAM) Trust Framework Provider Adoption Process (TFPAP) should be used. Components should see www.IDmanagement.gov for details regarding the Federal Identity, Credentialing, and Access Management (FICAM) initiative.

E-authentication guidance is provided in the following:

- OMB M-0404, *E-Authentication Guidance for Federal Agencies*
- NIST SP 800-63, *Electronic Authentication Guideline*

Policy ID	DHS Policy Statements	Relevant Controls
3.14.7.a	For systems that allow online transactions, Components shall determine whether e-authentication requirements apply.	IA-2
3.14.7.b	Components shall determine the appropriate assurance level for e-authentication by following the steps described in OMB M-04-04, *E-Authentication Guidance for Federal Agencies*.	IA-2
3.14.7.c	Components shall implement the technical requirements described in NIST SP 800-63, *Electronic Authentication Guideline*, at the appropriate assurance level for those systems with e-authentication requirements.	IA-2
3.14.7.d	Components shall ensure that each SP reflects the e-authentication status of the respective system.	IA-2, PL-2
3.14.7.e	Programs considering the use of e-authentication are required to conduct a PTA to initiate the review of privacy risks and how they will be mitigated.	PL-5
3.14.7.f	Existing physical and logical access control systems shall be upgraded to use PIV credentials, in accordance with NIST and DHS guidelines.	
3.14.7.g	All new systems under development shall be enabled to use PIV credentials, in accordance with NIST and DHS guidelines, prior to being made operational.	

3.15 DHS CFO Designated Systems

DHS CFO Designated Systems are systems that require additional management accountability to ensure effective internal control exists over financial reporting. The DHS CFO publishes the approved list of CFO Designated Systems annually. This section provides additional requirements for these systems based on OMB Circular A-123, *Management's Responsibility for Internal Control (A-123),* Appendix A. The requirements contained in OMB Circular A-123 have been mapped to the NIST SP 800-53 controls and documented in DHS 4300A Attachment R. These requirements are in addition to the other security requirements established in this document and other CFO developed financial system Line of Business requirements. *Wherever*

there is a conflict between this and other sections of this policy regarding requirements for CFO Designated Systems, this section takes precedence.

These additional requirements provide a strengthened assessment process and form the basis for management's assurance on the internal control over financial reporting. The strengthened process requires management to document the design and test the operating effectiveness of controls for CFO Designated Systems. The system owner is responsible for ensuring that all requirements, including security requirements, are implemented on DHS systems. Component CISOs/ISSMs must coordinate with their CFO organization to ensure that these requirements are implemented.

Policy ID	DHS Policy Statements	Relevant Controls
3.15.a	System owners are responsible for ensuring that security assessments of key security controls (i.e., Security Assessment and Security Assessment Report [SAR]) for CFO Designated Systems are completed annually in TAF. This includes updating the ST&E & SAR annually.	CA-2, CA-7
3.15.b	The DHS CFO shall designate the systems that must comply with additional internal controls and the Office of the CFO shall review and publish this list annually.	CA-2
3.15.c	Component CISOs/ISSMs shall ensure that vulnerability assessments and verification of critical patch installations are conducted on all CFO Designated Systems. Vulnerability assessment shall be performed at least annually.	RA-5
3.15.d	All CFO Designated Systems shall be assigned a minimum impact level of "**moderate**" for confidentiality, integrity, and availability. If warranted by a risk based assessment, the integrity objective shall be elevated to "high."	RA-2
3.15.e	All Component security accreditations for CFO Designated Systems shall be approved and signed by the Component CFO.	CA-6
3.15.f	System Owners shall ensure that Contingency plans are created for *all* CFO Designated Systems requiring moderate availability and Disaster Recovery plans are created for *all* CFO Designated Systems requiring high availability and that each plan is tested annually.	CP-2, CP-4
3.15.g	Component CISOs/ISSMs shall ensure that weekly incident response tracking is performed for all of their respective CFO Designated Systems.	IR-5
3.15.h	Component CISOs/ISSMs shall ensure that incidents related to their respective CFO Designated Systems are reported to the Component CFO.	IR-4, IR-6
3.15.i	The SP shall be updated for CFO Designated Systems at least annually. Key controls prescribed in Attachment R, *Compliance Framework for CFO Designated Systems* shall be identified in the SP.	PL-2

Policy ID	DHS Policy Statements	Relevant Controls
3.15.j	Component CISOs/ISSMs must request a waiver or exception from the DHS CISO if a key control weakness is identified for a CFO Designated System and not remediated within twelve (12) months.	CA-5, CA-7
3.15.k	Component CFOs shall ensure that a fulltime dedicated ISSO is assigned to each CFO Designated System. CFO Designated System ISSOs may be assigned to more than one CFO Designated System.	---
3.15.l	CFO Designated System ATOs shall be rescinded if Components fail to comply with testing and reporting requirements established within this policy.	CA-1, CA-6
3.15.m	Component CFOs shall work with their Component CISOs/ISSMs to approve any major system changes to CFO Designated Systems identified in the DHS inventory.	CA-1, CM-8

3.16 Social Media

Social Media hosts are public, content sharing Web sites that allow individual users to upload, view and share content such as video clips, press releases, opinions and other information. The DHS Office of Public Affairs (OPA) will publish Terms of Service (TOS) and guidelines for posting to these sites. In some cases the Department will develop its own and in other cases will endorse those of other Federal agencies, such as the General Services Administration (GSA) or Office of Personnel Management (OPM). Due to the high threat of malware, Social Media host sites have been blocked at the TIC.

Policy ID	DHS Policy Statements	Relevant Controls
3.16.a	Only OPA designated content managers (Department level and Component level) may post content, and only those individuals designated by OPA for this purpose shall be granted access on a continuing basis.	SA-6
3.16.b	Posted content shall be in keeping with the Department's Terms of Service (TOS) and guidelines for a given social media host (e.g., YouTube, Twitter). This condition is also met if the Department endorses another appropriate Federal agency's guidance or TOS (e.g., GSA, OPM). Under no circumstances shall sensitive information be posted to social media sites.	---
3.16.c	Content shall not be posted to any social media site for which the Department has not approved and published final posting guidelines *and* TOS.	SA-6
3.16.d	Content managers shall review and understand the appropriate Department-level TOS for the appropriate social media host.	---

Policy ID	DHS Policy Statements	Relevant Controls
3.16.e	Content managers shall make a risk decision prior to posting any information and shall recognize that social medial hosts are not DHS information systems and therefore subject only to the DHS TOS and not to DHS policy. Once released, information is no longer under DHS control.	---

There are a number of security technologies that are especially important to consider when dealing with social media issues. These include:

- Trusted Internet Connections (TIC) – Section 5.4.4
- Host Configuration and Hardening – Section 4.8.4
- Enterprise Operations Center (EOC) and Network Operations Center (NOC) – Section 4.9
- Two-Factor Authentication – Section 5.4.1
- Domain Name System Security Extensions (DNSSEC) Capabilities – Section 5.4.3
- Trust Zones – Section 5.4.3
- Signed Code – Section 5.4.5
- Patching and Anti-Virus – Section 5.6

3.17 Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) addresses the privacy of individuals' health information by establishing a Federal privacy standard for health information and how it can be used and disclosed.

HIPAA prohibits the use or disclosure of Protected Health Information (PHI), electronic and otherwise, for any purpose other than treatment, payment, or health care operations without the authorization of the individual or as part of an exception within HIPAA.

Because of the diverse mission of DHS, it may be necessary for some Components to collect PHI as part of a larger mission requirement. (e.g. detainee processing, disaster relief). This section applies to all Components and personnel who collect, process, or store PHI (refer to NIST SP 800-66 for further information).

Policy ID	DHS Policy Statements	Relevant Controls
3.17.a	For those Components whose systems collect, process, or store Protected Health Information (PHI), they shall ensure that the stored information is appropriately protected in compliance with HIPAA and that access or disclosure is limited to the minimum required.	---
3.17.b	Covered Components shall work with the DHS Privacy Office, Component Privacy Office, or PPOC to ensure that privacy and disclosure policies comply with HIPAA requirements.	---

Policy ID	DHS Policy Statements	Relevant Controls
3.17.c	Covered Components shall ensure that employees with access to DHS systems that collect, process, or store PHI are trained on HIPAA requirements.	---
3.17.d	Covered Components shall establish administrative processes that can respond to complaints, requests for corrections of health information, and track disclosures of PHI.	---
3.17.e	When collecting PHI, Components shall issue a privacy notice to individuals concerning the use and disclosure of their PHI.	---

4.0 OPERATIONAL POLICIES

4.1 Personnel

DHS systems face threats from a myriad of sources. The intentional and unintentional actions of system users can potentially harm or disrupt DHS systems and facilities and could result in the destruction or modification of the data being processed, denial of service, and unauthorized disclosure of data. It is thus highly important that stringent safeguards be taken to reduce the risk associated with these types of threats.

4.1.1 Citizenship, Personnel Screening, and Position Categorization

Policy ID	DHS Policy Statements	Relevant Controls
4.1.1.a	Components shall designate the position sensitivity level for all Government and contractor positions that use, develop, operate, or maintain information systems and shall determine risk levels for each contractor position. Position sensitivity levels shall be reviewed annually and revised as appropriate.	PS-2, PS-3, PS-7
4.1.1.b	Components shall ensure the incumbents of these positions have favorably adjudicated background investigations commensurate with the defined position sensitivity levels.	PS-2, PS-3, PS-7
4.1.1.c	Components shall ensure that no Federal employee is granted access to DHS systems without having a favorably adjudicated Minimum Background Investigation (MBI) as defined in DHS Instruction 121-01-007, *Personnel Suitability and Security Program.* Active duty United States Coast Guard and other personnel subject to the Uniform Code of Military Justice shall be exempted from this requirement.	PS-3
4.1.1.d	Components shall ensure that no contractor personnel shall be granted access to DHS systems without having a favorably adjudicated Background Investigation (BI) as defined in DHS Instruction 121-01-007, *Suitability Screening Requirements for Contractor Employees* and the Department of Homeland Security Acquisition Regulation (HSAR).	PS-3
4.1.1.e	Components shall ensure that only U.S. Citizens are granted access to DHS systems and networks. Exceptions to the U.S. Citizenship requirement may be granted by the Component Head or designee with the concurrence of the Office of Security and the DHS CIO, in accordance with Section 1.5.4, U.S. Citizen Exception Requests, of this policy.	PS-3

4.1.2 Rules of Behavior

Policy ID	DHS Policy Statements	Relevant Controls
4.1.2.a	Components shall ensure that rules of behavior contain acknowledgement that the user has no expectation of privacy (a "Consent to Monitor" provision) and that disciplinary actions may result from violations.	PL-4
4.1.2.b	Components shall ensure that DHS users are trained regarding rules of behavior and that each user signs a copy prior to being granted user accounts or access to information systems or data.	AT-1, AT-2, PL-4

4.1.3 Access to Sensitive Information

Policy ID	DHS Policy Statements	Relevant Controls
4.1.3.a	System Owners shall ensure that users of the information systems supporting their programs have a valid requirement to access these systems.	AC-2

4.1.4 Separation of Duties

Separation of duties is intended to prevent a single individual from being able to disrupt or corrupt a critical security process.

Policy ID	DHS Policy Statements	Relevant Controls
4.1.4.a	Components shall divide and separate duties and responsibilities of critical information system functions among different individuals to minimize the possibility that any one individual would have the necessary authority or system access to be able to engage in fraudulent or criminal activity.	AC-2
4.1.4.b	All individuals requiring administrator privileges shall be reviewed and approved by the appropriate AO. The AO may delegate this duty to the appropriate system owner or Program Manager.	AC-2
4.1.4.c	Individuals requiring administrator privileges shall be assigned administrator accounts separate from their normal user accounts.	AC-6
4.1.4.d	Administrator accounts shall be used only for performing required administrator duties. Individuals shall use their regular user accounts to perform all other functions not directly tied to administrator duties (checking email, accessing the Internet).	AC-6

4.1.5 Information Security Awareness, Training, and Education

Policy ID	DHS Policy Statements	Relevant Controls
4.1.5.a	Components shall establish an information security training program for users of DHS information systems.	AT-1
4.1.5.b	DHS personnel, contractors, or others working on behalf of DHS accessing DHS systems shall receive initial training and annual refresher training, in security awareness and accepted security practices. Personnel shall complete security awareness within twenty-four (24) hours of being granted a user account. If the user fails to comply, user access shall be suspended.	AT-1, AT-4
4.1.5.c	DHS personnel, contractors, or others working on behalf of DHS with significant security responsibilities (e.g., ISSOs, system administrators) shall receive initial specialized training, and annual refresher training thereafter, specific to their security responsibilities.	AT-3
4.1.5.d	Components shall maintain training records, to include name and position, type of training received, and costs of training.	AT-4
4.1.5.e	User accounts and access privileges, including access to email, shall be disabled for those DHS employees who have not received annual refresher training unless a waiver is granted by the Component CISO/ISSM.	AT-1
4.1.5.f	Components shall prepare and submit an annual security awareness training plan, as specified by the DHS Information Security Training Program Office.	AT-1
4.1.5.g	Components shall prepare and submit information security awareness reports with content, frequency, format, and distribution as specified by the DHS CISO.	AT-1
4.1.5.h	Components shall provide evidence of training by submitting copies of training schedules, training rosters, and training reports, upon request of the DHS Information Security Training Program Office.	AT-4
4.1.5.i	The DHS CISO shall review Component information security awareness programs annually.	AT-1

4.1.6 Separation From Duty

Policy ID	DHS Policy Statements	Relevant Controls
4.1.6.a	Components shall implement procedures to ensure that system accesses are revoked for DHS employees, contractors, or others working on behalf of DHS who leave the Component, are reassigned to other duties, or no longer require access.	AC-2

Policy ID	DHS Policy Statements	Relevant Controls
4.1.6.b	Components shall establish procedures to ensure that all DHS information system-related property and assets are recovered from the departing individual and that sensitive information stored on any media is transferred to an authorized individual.	PS-4
4.1.6.c	Accounts for personnel on extended absences shall be temporarily suspended.	AC-2
4.1.6.d	System Owners shall review information system accounts supporting their programs at least annually.	AC-2

4.2 Physical Security

4.2.1 General Physical Access

Policy ID	DHS Policy Statements	Relevant Controls
4.2.1.a	Access to DHS buildings, rooms, work areas, spaces, and structures housing information systems, equipment, and data shall be limited to authorized personnel.	PE-2
4.2.1.b	Controls for deterring, detecting, restricting, and regulating access to sensitive areas shall be in place and shall be sufficient to safeguard against possible loss, theft, destruction, damage, hazardous conditions, fire, malicious actions, and natural disasters.	PE-3
4.2.1.c	Controls shall be based on the level of classification and risk, determined in accordance with Departmental security policy as reflected in this and other relevant documents.	PE-1, PM-9
4.2.1.d	Visitors shall sign in upon entering DHS facilities that house information systems, equipment, and data, be escorted during their stay, and sign out upon leaving. Non-DHS contractor or vendor access shall be limited to those work areas requiring their presence. Visitor logs shall be maintained and available for review for one (1) year.	PE-7
4.2.1.e	These requirements shall extend to DHS assets, located at non-DHS facilities or non-DHS assets and equipment hosting DHS data.	---

4.2.2 Sensitive Facility

Policy ID	DHS Policy Statements	Relevant Controls
4.2.2.a	Facilities processing, transmitting, or storing sensitive information shall incorporate physical protection measures based on the level of risk. The risk shall be determined in accordance with Departmental security policy as reflected in this and other relevant documents.	PE-1, PM-9

4.3 Media Controls

4.3.1 Media Protection

Policy ID	DHS Policy Statements	Relevant Controls
4.3.1.a	Components shall ensure that all media containing sensitive information, including hard copy media, backup media, and removable media such as USB drives, are stored in a secure location (e.g., a locked office, room, desk, bookcase, file cabinet, locked tape device, or other storage prohibiting access by unauthorized persons) when not in use.	MP-2, MP-4, PE-1
4.3.1.b	Components shall ensure that all offsite backup media are protected as per guidance in this section.	CP-6
4.3.1.c	DHS personnel, contractors, and others working on behalf of DHS are prohibited from using any non-Government issued removable media (USB drives, in particular) or connecting them to DHS equipment or networks or to store DHS sensitive information.	MP-2
4.3.1.d	Systems requiring encryption shall comply with Section 5.5.1, Encryption, of this policy. DHS-owned USB drives shall use encryption.	IA-7, SC-13
4.3.1.e	DHS-owned removable media shall not be connected to any non-DHS information system unless the AO has determined the acceptable level of risk based on compensating controls, published acceptable use guidance and the guidance has been approved by the respective CISO/ISSM. (The respective CISO is the CISO with that system in his or her inventory.)	AC-20, MP-2, PM-9
4.3.1.f	DHS-owned USB removable media shall not be connected to any non-DHS information system.	AC-20, MP-2
4.3.1.g	Components shall follow established procedures to ensure that paper and electronic outputs from systems containing sensitive information are protected.	MP-1
4.3.1.h	Users shall ensure proper protection of printed output. Printing of sensitive documents shall occur only when a trusted person is attending the printer.	SI-12

Policy ID	DHS Policy Statements	Relevant Controls
4.3.1.i	Components shall follow the procedures established by DHS MD 11042.1, *Safeguarding Sensitive But Unclassified (For Official Use Only) Information*, for the transportation or mailing of sensitive media.	MP-5

4.3.2 Media Marking and Transport

Policy ID	DHS Policy Statements	Relevant Controls
4.3.2.a	Media determined by the information owner to contain sensitive information shall be appropriately marked in accordance with DHS MD 11042.1, *Safeguarding Sensitive But Unclassified (For Official Use Only) Information*.	MP-3
4.3.2.b	Components shall control the transport of information system media containing sensitive data, outside of controlled areas and restrict the pickup, receipt, transfer, and delivery to authorized personnel.	MP-5

4.3.3 Media Sanitization and Disposal

Policy ID	DHS Policy Statements	Relevant Controls
4.3.3.a	Components shall ensure that any information systems storage medium containing sensitive information is sanitized using approved sanitization methods before it is disposed of, reused, recycled, or returned to the owner or manufacturer.	MP-6
4.3.3.b	Components shall maintain records of the sanitization and disposition of information systems storage media.	MP-6
4.3.3.c	Components shall periodically test degaussing equipment to verify that the equipment is functioning properly.	MP-6

4.3.4 Production, Input/Output Controls

Policy ID	DHS Policy Statements	Relevant Controls
4.3.4.a	Components shall follow established procedures to ensure that sensitive information cannot be accessed or stolen by unauthorized individuals.	SI-12
4.3.4.b	These procedures shall address not only the paper and electronic outputs from systems but also the transportation or mailing of sensitive media.	SI-12

4.4 Voice Communications Security

4.4.1 Private Branch Exchange

Policy ID	DHS Policy Statements	Relevant Controls
4.4.1.a	Components shall provide adequate physical and information security for all DHS-owned Private Branch Exchanges (PBX). (Refer to NIST SP 800-24, *PBX Vulnerability Analysis*, for guidance on detecting and fixing vulnerabilities in PBX systems.)	CM-2

4.4.2 Telephone Communications

Policy ID	DHS Policy Statements	Relevant Controls
4.4.2.a	Components shall develop guidance for discussing sensitive information over the telephone. Guidance shall be approved by a senior Component official and is subject to review and approval by the DHS CISO. Under no circumstances shall classified national security information be discussed over unsecured telephones.	PL-4

4.4.3 Voice Mail

Policy ID	DHS Policy Statements	Relevant Controls
4.4.3.a	Sensitive information shall not be communicated over nor stored in voice mail.	PL-4

4.5 Data Communications

4.5.1 Telecommunications Protection Techniques

Policy ID	DHS Policy Statements	Relevant Controls
4.5.1.a	Components shall carefully select the telecommunications protection techniques that meet their information security needs, in the most cost-effective manner, consistent with Departmental and Component information system security policies. Approved protected network services (PNS) may be used as cost-effective alternatives to the use of encryption for sensitive information requiring telecommunications protection.	CM-2

4.5.2 Facsimiles

Policy ID	DHS Policy Statements	Relevant Controls
4.5.2.a	Components shall implement and enforce technical controls for fax technology and systems (including fax machines, servers, gateways, software, and protocols) that transmit and receive sensitive information.	SC-1, SC-7, SC-8, SC-9
4.5.2.b	Components shall configure fax servers to ensure that incoming lines cannot be used to access the network or any data on the fax server.	AC-4

4.5.3 Video Teleconferencing

Policy ID	DHS Policy Statements	Relevant Controls
4.5.3.a	Components shall implement controls to ensure that only authorized individuals are able to participate in each videoconference.	AC-3, PE-3
4.5.3.b	Components shall ensure that appropriate transmission protections, commensurate with the highest sensitivity of information to be discussed, are in place throughout any video teleconference.	SC-8, SC-9
4.5.3.c	Video teleconferencing equipment and software shall be disabled when not in use.	AC-3, PE-3

4.5.4 Voice Over Data Networks

Voice over Internet Protocol (VoIP) and similar technologies move voice over digital networks. These technologies use protocols originally designed for data networking. Such technologies include Voice over Frame Relay, Voice over Asynchronous Transfer Mode, and Voice over Digital Subscriber Line (refer to NIST SP 800-58 for further information).

Policy ID	DHS Policy Statements	Relevant Controls
4.5.4.a	Prior to implementing voice over data network technology, Components shall conduct rigorous risk assessments and security testing and provide a business justification for their use. Any systems that employ this technology shall be accredited for this purpose with residual risks clearly identified.	SC-19, PM-9
4.5.4.b	Voice over data network implementations shall have sufficient redundancy to ensure network outages do not result in the loss of both voice and data communications.	SC-19
4.5.4.c	Components shall ensure appropriate identification and authentication controls, audit logging, and integrity controls are implemented on every element of their voice over data networks.	SC-19

Policy ID	DHS Policy Statements	Relevant Controls
4.5.4.d	Components shall ensure that physical access to voice over data network elements is restricted to authorized personnel.	SC-19

4.6 Wireless Network Communications

Wireless network communications technologies include the following:

- Wireless systems (e.g., wireless local area networks [WLAN], wireless wide area networks [WWAN], wireless personal area networks [WPAN], peer-to-peer wireless networks, information systems that leverage commercial wireless services). Wireless systems include the transmission medium, stationary integrated devices, firmware, supporting services, and protocols
- Wireless portable electronic devices (PED) capable of storing, processing, or transmitting sensitive information (e.g., personal digital assistants [PDA], smart telephones, two-way pagers, handheld radios, cellular telephones, personal communications services [PCS] devices, multifunctional wireless devices, portable audio/video recording devices with wireless capability, scanning devices, messaging devices)
- Wireless tactical systems, including mission-critical communication systems and devices (e.g., include Land Mobile Radio [LMR] subscriber devices and infrastructure equipment, remote sensors, technical investigative communications systems)
- Radio Frequency Identification (RFID)

Policy ID	DHS Policy Statements	Relevant Controls
4.6.a	Wireless network communications technologies are prohibited from use within DHS unless the appropriate AO specifically approves a technology and application.	AC-18
4.6.b	Components using Public Key Infrastructure (PKI)-based encryption on wireless systems, wireless PEDs, and wireless tactical systems shall implement and maintain a key management plan approved by the DHS PKI Policy Authority.	IA-5, SC-12

4.6.1 Wireless Systems

Wireless system policy and procedures are described more completely in Attachment Q1 (*Wireless Systems*) to the DHS 4300A *Sensitive Systems Handbook.*

Policy ID	DHS Policy Statements	Relevant Controls
4.6.1.a	Annual information security assessments shall be conducted on all approved wireless systems. Wireless information security assessments shall enumerate vulnerabilities, risk statements, risk levels, and corrective actions.	CA-2, PM-9
4.6.1.b	A POA&M shall be developed to address wireless information security vulnerabilities. These plans shall prioritize corrective actions and implementation milestones in accordance with defined risk levels.	CA-5, PM-4, PM-9
4.6.1.c	Components shall identify countermeasures to denial-of-service attacks and complete a risk based evaluation prior to approving the use of a wireless PED	AC-19, PM-9, SC-5
4.6.1.d	SPs shall adopt a defense-in-depth strategy that integrates firewalls, screening routers, wireless intrusion detection systems, antivirus software, encryption, strong authentication, and cryptographic key management to ensure information security solutions and secure connections to external interfaces are consistently enforced.	SI-3
4.6.1.e	Legacy wireless systems that are not compliant with DHS information security policy shall implement a migration plan to outline the provisions, procedures, and restrictions for transitioning these systems to DHS-compliant security architectures. Operation of these noncompliant systems requires an approved waiver or exception to policy from the DHS CISO.	CA-5
4.6.1.f	Component CISOs shall review all system applications for wireless usage, maintain an inventory of systems, and provide that inventory to the DHS CISO annually.	AC-18, PM-5
4.6.1.g	Component CISOs shall (i) establish usage restrictions and implementation guidance for wireless technologies; and (ii) authorize, monitor, and control wireless access to DHS information systems.	AC-18

4.6.2 Wireless Portable Electronic Devices

Wireless PEDs include PDAs, smart telephones, two-way pagers, handheld radios, cellular telephones, PCS devices, multifunctional wireless devices, portable audio/video recording devices with wireless capability, scanning devices, messaging devices, and any other wireless clients capable of storing, processing, or transmitting sensitive information.

Wireless PED policy and procedures are described more completely in Attachment Q2 (*Wireless Portable Electronic Devices*) to the DHS 4300A *Sensitive Systems Handbook*.

Policy ID	DHS Policy Statements	Relevant Controls
4.6.2.a	The use of wireless PEDs and accessory devices in areas where sensitive or classified information is discussed, maintained, or distributed is prohibited unless specifically authorized by the AO in writing.	AC-19, PL-4
4.6.2.b	Wireless PEDs shall not be tethered or otherwise physically or wirelessly connected to the DHS-wired core network without written consent from the AO.	AC-18, AC-19
4.6.2.c	Wireless PEDs shall not be used to store, process, or transmit combinations, personal identification numbers (PIN), or sensitive information in unencrypted formats.	AC-19, IA-5, IA-7
4.6.2.d	Wireless PEDs such as BlackBerry devices and smart phones shall implement strong authentication, data encryption, and transmission encryption technologies. Portable electronic devices such as BlackBerry devices and smart phones shall be password-protected, with a security timeout period established. For BlackBerry devices, the security timeout shall be set to ten (10) minutes.	AC-19, IA-7, SC-8, SC-9, SC-13
4.6.2.e	SPs shall promulgate the provisions, procedures, and restrictions for using wireless PEDs to download mobile code in an approved manner.	SC-18
4.6.2.f	Wireless PEDs shall be operated only when current DHS TRM-approved versions of antivirus software and software patches are installed.	SI-3
4.6.2.g	Cost-effective countermeasures to denial-of-service attacks shall be identified and established prior to a wireless PED being approved for use.	SC-5 SC-7
4.6.2.h	Components shall maintain a current inventory of all approved wireless PEDs in operation.	PM-5
4.6.2.i	Wireless PEDs shall be cleared of all information before being reused by another individual, office, or Component within DHS or before they are surplused; wireless PEDs that are being disposed of, recycled, or returned to the owner or manufacturer shall first be sanitized using approved procedures.	MP-6
4.6.2.j	Legacy wireless PEDs that are not compliant with DHS information security policy shall implement a migration plan that outlines the provisions, procedures, and restrictions for transitioning these wireless PEDs to DHS-compliant security architectures. Operation of these noncompliant systems requires an approved waiver or exception from the DHS CISO.	CA-5 CA-6
4.6.2.k	Components shall ensure that personally owned PEDs and Government-owned PEDs not authorized to process classified information are not permitted in conference rooms or secure facilities where classified information is discussed.	AC-19, PE-18

Policy ID	DHS Policy Statements	Relevant Controls
4.6.2.l	The AO shall approve the use of Government-owned PEDs to process, store, or transmit sensitive information.	CA-6
4.6.2.m	The use of add-on devices, such as cameras and recorders, is not authorized unless approved by the AO. Functions that can record or transmit sensitive information via video, Infrared (IR), or Radio Frequency (RF) shall be disabled in areas where sensitive information is discussed.	AC-19, CM-7, PE-18, SC-7

4.6.2.1 Cellular Phones

Policy ID	DHS Policy Statements	Relevant Controls
4.6.2.1.a	Components shall develop guidance for discussing sensitive information on cellular phones. Guidance shall be approved by a senior Component official and is subject to review by the DHS CISO. Under no circumstances shall classified information be discussed on cellular phones.	PL-4

4.6.2.2 Pagers

Policy ID	DHS Policy Statements	Relevant Controls
4.6.2.2.a	Pagers shall not be used to transmit sensitive information.	PL-4

4.6.2.3 Multifunctional Wireless Devices

Wireless devices have evolved to be multifunctional (cell phones, pagers, and radios can surf the Internet, retrieve email, take and transmit pictures). Most of these functions do not have sufficient security.

Policy ID	DHS Policy Statements	Relevant Controls
4.6.2.3.a	Functions that cannot be encrypted using approved cryptographic modules shall not be used to process, store, or transmit sensitive information.	AC-19, SC-8, SC-9, SC-12
4.6.2.3.b	Functions that transmit or receive video, IR, or radio frequency RF)signals shall be disabled in areas where sensitive information is discussed.	AC-19, PE-18
4.6.2.3.c	Short Message Service (SMS) and Multimedia Messaging Service (MMS) shall not be used to process, store, or transmit sensitive information, and shall be disabled whenever possible.	---

4.6.3 Wireless Tactical Systems

Wireless tactical systems include LMR subscriber devices, infrastructure equipment, remote sensors, and technical investigative communications systems. Because they are often deployed under circumstances in which officer safety and mission success are at stake, wireless tactical systems require even greater security measures. To ensure secure tactical communications, Components must implement strong identification, authentication, and encryption protocols designed specifically for each wireless tactical system.

Wireless tactical system policy and procedures are described more completely in Attachment Q3 (*Wireless Tactical Systems*) to the DHS 4300A *Sensitive Systems Handbook*.

Policy ID	DHS Policy Statements	Relevant Controls
4.6.3.a	AOs shall be immediately notified when any security features are disabled in response to time-sensitive, mission-critical incidents.	CM-3
4.6.3.b	Wireless tactical systems shall implement strong identification, authentication, and encryption.	IA-2, IA-7, SC-8, SC-9
4.6.3.c	Cost-effective countermeasures to denial-of-service attacks shall be identified and established prior to a wireless tactical system being approved for use.	SC-5
4.6.3.d	Components shall maintain a current inventory of all approved wireless tactical systems in operation.	PM-5
4.6.3.e	Legacy tactical wireless systems that are not compliant with DHS information security policy shall implement a migration plan to outline the provisions, procedures, and restrictions for transitioning these systems to DHS-compliant security architectures. Operation of these noncompliant systems requires an approved waiver or exception from the DHS CISO, as appropriate.	---
4.6.3.f	The security configuration of LMR subscriber units shall be validated via over-the-air-rekeying (OTAR) or hard rekey using a crypto-period no longer than 180 days.	SC-12
4.6.3.g	All LMR systems shall comply with Project 25 (P25, EIA/TIA-102) security standards where applicable.	CM-2

4.6.4 Radio Frequency Identification

Radio Frequency Identification (RFID) enables wireless identification of objects over significant distances. Because of the computing limitations of RFID tags, it often is not feasible to implement many of the security mechanisms, such as cryptography and strong authentication that are commonly supported on personal workstations, servers, and network infrastructure devices. RFID security controls can support Departmental and Component privacy objectives, mitigate risks to business processes, and prevent the disclosure of sensitive data.

RFID policy and procedures are described more completely in Attachment Q4 (S*ensitive RFID Systems*) to the DHS 4300A *Sensitive Systems Handbook.*

Policy ID	DHS Policy Statements	Relevant Controls
4.6.4.a	Components implementing RFID systems shall assess hazards of electromagnetic radiation to fuel, ordinance, and personnel before deployment of the RFID technology.	PE-18
4.6.4.b	Components shall limit data stored on RFID tags to the greatest extent possible, recording information beyond an identifier only when required for the application mission. When data beyond an identifier is stored on a tag, the tag's memory shall be protected by access control.	AC-6, PL-5
4.6.4.c	Components shall develop a contingency plan, such as the use of a fallback identification technology, to implement in case of an RFID security breach or system failure.	---
4.6.4.d	Components shall identify and implement appropriate operational and technical controls to limit unauthorized tracking or targeting of RFID-tagged items when these items are expected to travel outside the Component's physical perimeter.	AC-14
4.6.4.e	When the RFID system is connected to a DHS data network, Components shall implement network security controls to segregate RFID network elements such as RFID readers, middleware, and databases from other non-RFID network hosts.	CM-6
4.6.4.f	Components implementing RFID technology shall determine whether or not tag cloning is a significant business risk. If such a significant risk exists, then tag transactions shall be cryptographically authenticated.	IA-7, PM-9, RA-3

4.7 Overseas Communications

Policy ID	DHS Policy Statements	Relevant Controls
4.7.a	Where required or appropriate, all communications outside of the United States and its territories shall be in accordance with the Department of State Foreign Affairs Manual (FAM), 12 FAM 600, *Information Security Technology*.	---

4.8 Equipment

4.8.1 Workstations

Policy ID	DHS Policy Statements	Relevant Controls
4.8.1.a	Components shall configure *workstations* to either log off, or activate a password-protected lock, or password-protected screensaver within fifteen (15) minutes of user inactivity.	AC-11, CM-6
4.8.1.b	Components shall ensure that workstations are protected from theft.	PE-3
4.8.1.c	Users shall either log off or lock their workstations when unattended.	---

4.8.2 Laptop Computers and Other Mobile Computing Devices

Policy ID	DHS Policy Statements	Relevant Controls
4.8.2.a	Information stored on any laptop computer or other mobile computing device that may be used in a residence or on travel shall use encryption in accordance with Section 5.5.1, Encryption, for data at rest and in motion. Passwords, tokens and Smart Cards shall not be stored on or with the laptop or other mobile computing device.	AC-19, IA-2, SC-12
4.8.2.b	Laptop computers shall be powered down when not in use (due to volatile memory vulnerabilities).	AC-19, PL-4
4.8.2.c	Laptop computers and other mobile computing devices in offices shall be secured when unattended via a locking cable, locked office, or locked cabinet or desk.	AC-19, PE-3, PL-4
4.8.2.d	Users shall obtain the written approval of the office director before taking a laptop computer or other mobile computing device outside of the United States or its territories.	AC-19, PL-4

4.8.3 Personally Owned Equipment and Software

Policy ID	DHS Policy Statements	Relevant Controls
4.8.3.a	Personally owned equipment and software shall not be used to process, access, or store sensitive information without the written prior approval of the AO.	SA-6
4.8.3.b	Equipment that is not owned or leased by the Federal Government, or operated by a contractor on behalf of the Federal Government, shall not be connected to DHS equipment or networks without the written prior approval of the Component CISO/ISSM.	SA-9

Policy ID	DHS Policy Statements	Relevant Controls
4.8.3.c	Any device that has been obtained through civil or criminal asset forfeiture shall not be used as part of a DHS information system nor used to process DHS data.	AC-20

4.8.4 Hardware and Software

Policy ID	DHS Policy Statements	Relevant Controls
4.8.4.a	Components shall ensure that DHS information systems follow the hardening guides for operating systems and the configuration guides for applications promulgated by the DHS CISO. DHS Sensitive Systems Handbook, Enclosure 1, includes the DHS Secure Baseline Configuration Guides.	CM-2, CM-6
4.8.4.b	Components shall limit access to system software and hardware to authorized personnel.	AC-3, CM-5
4.8.4.c	Components shall test, authorize, and approve all new and revised software and hardware prior to implementation in accordance with their Configuration Management Plan.	CM-2, CM-3
4.8.4.d	Components shall manage systems to reduce vulnerabilities through vulnerability testing and management, promptly installing patches, and eliminating or disabling unnecessary services.	CM-3, RA-5
4.8.4.e	Components shall ensure that maintenance ports are disabled during normal system operation and enabled only during approved maintenance activities.	MA-1
4.8.4.f	System libraries shall be managed and maintained to protect privileged programs and to prevent or minimize the introduction of unauthorized code.	SI-7
4.8.4.g	Components shall develop maintenance policy and procedures.	MA-1
4.8.4.h	If cleared maintenance personnel are not available, a trusted DHS employee with sufficient technical knowledge to detect and prevent unauthorized modification to the information system or its network shall monitor and escort the maintenance personnel during maintenance activities. This situation shall only occur in exceptional cases. Components shall take all possible steps to ensure that trusted maintenance personnel are available.	MA-5
4.8.4.i	Maintenance using a different user's identity may be performed only when the user is present. The *user* shall log in and observe the maintenance actions at all times. *Users shall not share their authentication information with maintenance personnel.*	MA-5